IL04/00903

מדינת ישראל
STATE OF ISRAEL

Ministry of Justice
Patent Office

משרד המשפטים
לשכת הפטנטים

This is to certify that annexed hereto is a true copy of the documents as originally deposited with the patent application particulars of which are specified on the first page of the annex.

זאת לתעודה כי
רצופים בזה העתקים
נכונים של המסמכים
שהופקדו לכתחילה
עם הבקשה לפטנט
לפי הפרטים הרשומים
בעמוד הראשון של
הנספח.

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

This ....1.4.-10-.200... היום

ג. לשרי
על הבוחנים

רשם הפטנטים
Commissioner of Patents

נתאשר
Certified

לשימוש הלשכה
For Office Use

מספר: :Number	158158
תאריך: :Date	29-09-2003
הוקדם / נדחה: :Ante / Post-dated	

חוק הפטנטים, התשכ"ז - 1967
PATENTS LAW, 5727-1967

בקשה לפטנט
Application for Patent

אני, (שם המבקש, מענו - ולגבי גוף מאוגד - מקום התאגדותו)
I (Name and address of applicant, and, in case of body corporate place of incorporation)

Bamboo MediaCasting Ltd.
P.O. Box 5035
Kfar Saba 44150
Israel

במבו מדיהקסטינג בע"מ
ת.ד. 5035
כפר סבא 44150
ישראל

בעל אמצאה מכח הדין Law Owner, by virtue of
Of an invention, the title of which is ששמה הוא

(בעברית) (Hebrew) חלוקה של מידע למשתמשים על ערוץ משותף

(באנגלית) (English) Distribution of Multicast Data to Users

מבקש בזאת כי ינתן לי עליה פטנט
Hereby apply for a patent to be granted to me in respect therof

*בקשת חלוקה - Application of Division	*בקשת פטנט מוסף - Application for Patent Addition	*דרישה דין קדימה Priority Claim		
מבקשת פטנט from Application No. ________ מס' Dated ________ מיום	*לבקשה/לפטנט to Patent/Appl. No. ________ מס' Dated ________ מיום	מספר/ סימן Number/Mark	תאריך Date	מדינת האגוד Convention Country

*יפוי כח: [✓ כללי]/מיוחד - [✓ רצוף בזה]/ עוד יוגש
P.O.A: general / individual - attached / to be filed later
filed in case 154739 הוגש בעניין

המען למסירת הודעות ומסמכים בישראל
Address for Service in Israel
פנסטר ושות'
קניין רוחני 2002 בע"מ
רח' בזל 16 פ"ת
ת.ד. 10256 פ"ת, 49002

חתימת המבקש
Signature of Applicant
עבור המבקש,
פנסטר ושות'
קניין רוחני 2002 בע"מ

היום 29 בחודש ספטמבר שנת 2003
This 29 Of ספטמבר Of the year 2003

לשימוש הלשכה
For Office Use

279/03432

טופס זה, כשהוא מוטבע בחותם לשכת הפטנטים ומושלם מספר ובתאריך ההגשה, הינו אישור להגשת הבקשה שפרטיה רשומים לעיל.
This form, impressed with the Seal of the Patent Office and indicating the number and date of filing, certifies the filing of the application, the particulars of which are set out above.

חלוקה של מידע למשתמשים על ערוץ משותף

Distribution of Multicast Data to Users

במבו מדיהקסטינג בע״מ

Bamboo MediaCasting Ltd.
c:279/03432

DISTRIBUTION OF MULTICAST DATA TO USERS

FIELD OF THE INVENTION

The present invention relates generally to communication networks and particularly to methods of multicast transmission.

BACKGROUND OF THE INVENTION

Data transmission networks are used to provide different types of data. Some data, such as real time telephony, must be provided quickly, and it is acceptable if a small portion of the data is lost. For other types of data, such as executable programs and other files, an entire data file must be received without any loss. In the IP protocol suite, the UDP protocol is used for data requiring fast delivery, while TCP is used for data requiring reliable delivery (i.e., without any loss). In the TCP protocol, the receiver continuously transmits acknowledgements on the data it receives, and retransmissions are performed when data was not acknowledged.

When it is desired to provide the same data to many users, multicasting may be used, in order to reduce the bandwidth consumption. In multicasting, a single transmission is listened to by a plurality of receivers. It is generally not practical for each receiver to provide continuous acknowledgements of the multicast data directly to the transmitter. Various methods, such as described in U.S. Patent 5,541,927 by Kristol, Paul and Sabnani and in U.S. patent 6,269,080 to Kumar, the disclosures of which are incorporated herein by reference, were suggested to reduce the number of acknowledgements transmitted to the transmitter, by designating one or more representative acknowledgement providers. In addition, it has been suggested, for example in U.S. patent 5,727,002, the disclosure of which is incorporated herein by reference, to use a NAK acknowledgement method, in which receivers send acknowledgements only for data they did not receive.

Generally, when a packet was not received by one or more of the receivers, the sender re-multicasts the packet to all the receivers. In some cases, however, when only a single receiver needs to receive a retransmission, the packet is transmitted to that receiver on a point-to-point connection, if such a connection is available.

Cellular phones can be used for receiving video clips and other data, in addition to their use for point to point telephone communication. Multicasting the data to the cellular phones or to other mobile stations allows efficient use of the available bandwidth, such that large amounts of data can be provided to the cellular phones without requiring prohibitive amounts of bandwidth. In some cases, users are required to subscribe to a multicast service if they desire to receive the data. Upon subscribing, the users receive a decoding key which they use in decoding the multicast data. The key may be changed periodically in order to prevent users terminating their subscription from being able to decode data transmitted after the end of their subscription period.

A user does not always want to subscribe for a service for a long duration. For example, in some cases it may be desired to allow users to pay for each piece of data they receive, separately. In order to provide a reliable service, it is important to bill clients only if they actually received the multicast data. In addition, in order to maximize revenues it is desired to maximize the number of users receiving the multicast data.

In some networks, most users are generally continuously listening to the multicast channel, such that a multicast message may be transmitted to the users, if desired, without previous notice. In other networks, however, the receivers are not continuously tuned onto the multicast channel and the receivers must be notified about the transmission in order to tune onto the channel at the designated time. Mobile stations, for example, are generally assigned a wireless channel only when the data is actually transmitted, in order to conserve battery power and bandwidth. In such networks, the data source generally transmits a notification message to the mobile stations, instructing them to tune onto the multicast channel.

U.S. patent 6,453,438 to Miller et al., the disclosure of which is incorporated herein by reference, describes a method for managing multicast of data to receivers on a receiver list. The receivers on the list are notified on the upcoming data transmission and are requested to reply as to whether they will receive the data. Receivers responding that they will not be able to receive the transmission are added to a recovery list. At a later time, an attempt is made to provide the data to the receivers on the recovery list.

The transmission of multicast data in a cell of a cellular network generally requires higher power transmission levels than unicast data, in order to allow for all the receivers in the cell to receive the data. Higher transmission power levels consume more system resources, especially in noise-budget cellular networks (e.g., CDMA).

U.S. patent 6,360,076 to Segura et al., the disclosure of which is incorporated herein by reference, describes a method of adjusting the transmission power to the locations of the receivers in the cell. Thus, the power and/or bandwidth consumption may be reduced when the receivers are located, for example, close to the transmitter.

U.S. patent publication 2003/0007499 to Rajahalme, the disclosure of which is incorporated herein by reference, suggests determining whether to use multicast, unicast or a combination of multicast and unicast (i.e., some users receive the data in a multicast transmission, others in a unicast transmission) in providing data to subscribers within a specific cell. According to the '499 publication, broadcasting to the whole cell uses a lot of power and usually requires a robust channel coding, because there is no feedback possibility for the receivers to indicate lost frames. The '499 publication states that the invention is based on the premise that the membership of the group communication is known when allocating radio resources for the group communication delivery.

The combination of multicast and unicast is suggested for use when it would be cheapest to deliver the data by multicast, but some of the group members are not able to receive the broadcast for one reason or another. In other words, the multicast group is handled as subgroups to which the multicast packet is delivered using different methods.

SUMMARY OF THE INVENTION

A general aspect of the present invention relates to using less than optimal measures for delivering multicast data to receivers and supplementing receivers that did not receive the multicast data properly in point to point unicast transmissions.

An aspect of some embodiments of the invention relates to multicasting a data file to a list of receivers, in a network in which receivers are not continuously tuned to a multicast transmission channel. The method includes transmitting a notification on an upcoming multicast session, for example including the channel on which the multicast will be transmitted, to the receivers and performing the multicast session thereafter without receiving acknowledgements for the notification. It is noted that a receiver that did not receive the notification will not be able to receive the multicast transmission. Not using any acknowledgement measures for the notification may result in a lower percentage of receivers that receive the data file during the multicast transmission. In accordance with the present invention, the cost of unicasting the file to a larger number of receivers, due to the fact that they did not receive the file during multicast, is preferred over the cost of receiving acknowledgements from each of the receivers, for receiving the notification.

Optionally, the notification is transmitted several times in order to minimize the chances of a receiver not receiving the notification due to sporadic noise or a transient problem in the receiver. Alternatively or additionally, the notification is transmitted with a high protection level (e.g., a strong FEC). When the receivers are cellular units, the receivers that do not receive the notification are generally shut off or not located in a serviced cell and in most cases would not be able to receive the multicast transmission even if they received the notification.

In some embodiments of the invention, the file is delivered to each of the receivers on the list using at most a single application layer unicast connection for acknowledgement of data reception and receiving data portions not received during the multicast transmission. Optionally, beyond the single application layer unicast connection, no other transport layer (layer 4, e.g., TCP) connections are established for delivering the multicast file. In some embodiments of the invention, beyond the single application layer unicast connection, no other network layer (layer 3, e.g., IP) transmission is performed in relation to the delivery of the file.

In some of these embodiments, no acknowledgements (including negative acknowledgements) are transmitted during the data delivery. In some embodiments of the invention, the receivers cannot transmit acknowledgements unless a unicast connection is established between the receiver and a data server.

In some networks, receivers cannot transmit uplink messages to the transmitter while they are tuned onto the multicast channel. The switching between a multicast channel and a unicast channel required for uplink transmission is generally resource consuming and therefore it is desired to minimize the number of times a receiver switches between unicast and multicast channels. In addition, when there are a large number of receivers, it is desired to reduce the number of unicast connections established with the transmitter.

In some embodiments of the invention, the delivered file is encrypted with one or more keys. Optionally, the keys are provided to the receiver in a same unicast connection in which the receiver acknowledges receiving the entire data file and/or receives supplementary portions of the data file or the entire data file. Thus, the entire data file is provided to each of the users using a single unicast connection in addition to the multicast transmission.

Alternatively, the key is provided to at least some of the users in a unicast connection separate from the unicast connection used for acknowledgement and/or for data supplement. In accordance with this alternative, each receiver optionally uses at most two unicast connections to receive the data file and any data required for decoding the file. Optionally, no more than 10-20% of the receivers of the file use two unicast connections, while the remaining receivers use only a single unicast connection. The two unicast connections performed by some of the receivers are optionally performed consecutively without the receiver tuning onto the multicast channel between the unicast connections. This alternative is optionally used, for example, when the user reviews a portion of the received data before determining whether to view the rest of the data.

Optionally, beyond the two unicast connections, no other transport layer (layer 4, e.g., TCP) or even network layer (layer 3, e.g., IP) transmissions are performed in relation to the delivery of the file.

An aspect of some embodiments of the invention relates to multicasting a data file to a list of receivers, in which the file is delivered to each of the receivers on the list using at most a single application layer unicast connection for acknowledgement of data reception and receiving data portions not received during the multicast transmission.

An aspect of some embodiments of the invention relates to a method of multicast delivery of a data file to receivers. The method includes encoding the data file and providing one or more keys required for decoding the file only after the data is provided to the receiver. Providing the key only after the data is provided allows using the request for the key as an acknowledgment of receiving the file. In addition, providing the key only after the data transmission reduces the time available for users to illegally disseminate keys.

In some embodiments of the invention, the data file multicast to users includes a non-encrypted preview portion and at least one encrypted portion. The user may view the preview portion and accordingly determine whether to request the key for the encrypted portion. In some embodiments of the invention, the at least one encrypted portion may include a plurality of portions and the user may determine, independently from each other, for which portions to request decryption keys. Optionally, the user may request the key for each portion at different times. Alternatively or additionally, the user may determine whether to request a key for one of the portions based on viewing one or more of the portions for which a key was previously received. Providing a plurality of portions together reduces the amount of signaling required for the delivery of the plurality of portions to the receivers.

An aspect of some embodiments of the invention relates to a method of multicast delivery of a data file to receivers. The method includes estimating one or more transmission parameter values required to provide the multicast data, on the average, to a percentage of receivers lower than 100% and using the estimated parameter value for multicast transmission. The receivers that statistically do not receive the data during the multicast transmission are optionally provided the data in supplementary unicast transmissions. The percentage of receivers for which the transmission parameters are adjusted is selected so that the cost of providing the supplementary data in unicast is lower than the extra cost required for adjusting the transmission parameters at a higher level. Optionally, the estimation is adjusted to a level of reception of between about 90-95% of the receivers.

The estimation is optionally performed before each transmission, based on the current conditions (e.g., number of receivers, locations of receivers, noise level) of the network. Alternatively or additionally, the estimation is performed based on predetermined tests and/or assumptions for a plurality of transmissions.

The transmission parameters optionally include the transmission power used, the amount of redundancy used in the transmission, the transmission rate and/or any other parameter that affects the energy per bit of the transmission.

An aspect of some embodiments of the invention relates to a method of providing encrypted data to a receiver. The data is optionally provided by a first mobile network service provider, while the key for decrypting the data is provided by a second mobile network service provider. The first service provider optionally does not allocate the IP address used to receive the data. In some embodiments of the invention, the data is provided through a different gateway GPRS support node (GGSN) than the GGSN through which the key is provided.

In some embodiments of the invention, the data is provided in a multicast data delivery.

An aspect of some embodiments of the invention relates to a method of receiving multicast data, in which receivers are notified on an upcoming multicast session and then determine whether to tune onto the multicast channel on which the data is provided. Allowing the receivers to view the notification on a multicast session as a recommendation, rather than an instruction, allows the notification to be provided without specifically identifying the exact group of receivers to which the notification is directed. Thus, for example, when a file is transmitted a second time for those receivers that did not receive the file the first time, there is no need to identify the receivers that are to receive the second transmission in the notification, or to have the other receivers receive the file a second time.

In addition, the user may be queried whether to receive the data file after the notification is received, or may otherwise program the receiver on which files to receive, without involving the data server in the process.

In some embodiments of the invention, the receiver manages a table that indicates the multicast groups to which the receiver is subscribed. The receiver table is optionally managed in addition to a subscriber list managed by a transmission controller that provides the multicast data. Upon receiving the notification, the receiver determines the group or groups to which the data file referred to by the notification belongs and consults the table to determine whether to receive the data file. Alternatively, the user is queried. In some embodiments of the invention, the table indicates what is to be done if the user does not provide an answer (e.g., the user is not near the receiver, the receiver is powered off). In some embodiments of the invention, the rules on whether to receive a file, query the user and/or not receive a file may depend on one or more external parameters not related to the transmission (e.g., the time, date, location of the mobile) and/or one or more internal parameters related to the transmission (e.g., file size, planned transmission rate, expected error rate).

An aspect of some embodiments of the invention relates to a method of transmitting multicast data in a cellular network, in which different cells have different bandwidth allocated for the multicast transmission. The data is optionally provided to each of the base stations of the cells at a substantially same rate, and each base station transmits a portion of the data that it can transmit using its available bandwidth for the multicast transmission and drops data packets which they cannot transmit on their allocated bandwidth. The dropping of the packets is performed in a manner which substantially synchronizes the transmission of the non-dropped data packets of different base stations, such that the base stations transmit packets representing the same data content at substantially the same time. The term substantially synchronized refers herein to a gap of at most several packets (e.g., 3-5 packets) between the packets transmitted by different base stations and/or a time gap of at most a few seconds (e.g., 5-10 seconds) between the transmission of the same packet by different base stations.

Synchronizing the data transmission in the different cells, avoids the possibility of a mobile station moving from one cell to another during a multicast session, receiving the same data packets twice.

In some embodiments of the invention, the data packets are provided in groups and when a first packet of a new group is received, the base stations drop all the data they have of an old group. Optionally, the data source periodically transmits synchronization messages to the base stations, to keep the base stations synchronized. Alternatively or additionally, the base stations are configured to have small buffers and when the buffers are full, packets are dropped. In an exemplary embodiment of the invention, the buffers of the base stations have a small size, for example of between two to five packets, such that synchronization is maintained. Optionally, the buffers of substantially all the base stations have the same size.

In some embodiments of the invention, the data packets transmitted to the base stations are identical. Alternatively, different data packets, representing the same data content, are transmitted to different base stations.

There is therefore provided in accordance with an exemplary embodiment of the invention, a method of multicasting a data file, comprising transmitting a notification on an upcoming multicast transmission to a plurality of receivers designated to receive the multicast transmission, tuning by at least one of the plurality of receivers to a multicast channel, responsive to the notification, transmitting a data file, from a data server, on the multicast channel, without the data server receiving acknowledgements from the receivers on whether they received the notification, determining receivers designated to receive the multicast transmission that did not receive at least a portion of the data file and attempting to deliver the data file to the determined receivers.

Optionally, transmitting the notification comprises transmitting on a multicast or broadcast channel. Optionally, transmitting the notification comprises transmitting a unicast notification to each of the receivers on the designated receivers. Optionally, transmitting the notification comprises transmitting substantially only to designated receivers. Optionally, transmitting the notification comprises transmitting a message open also to non-designated receivers. Optionally, the notification indicates the channel on which the multicast transmission will be provided. Optionally, tuning to the multicast channel by at least one of the receivers comprises determining by each receiver that receives the notification whether to tune onto the multicast channel. Optionally, determining by each receiver that receives the notification whether to tune onto the multicast channel comprises determining, from the notification, a group to which the upcoming multicast transmission belongs and determining whether to tune to the multicast channel according to the determined group.

Optionally, determining by each receiver that receives the notification whether to tune onto the multicast channel comprises determining by consulting a list stored on the receiver.

Optionally, determining by each receiver that receives the notification whether to tune onto the multicast channel comprises determining based on input received from a user responsive to the notification. Optionally, the receivers do not transmit acknowledgements of reception of the notification, at all. Optionally, the receivers cannot transmit uplink messages to the data server, without stopping to listen to the multicast channel. Optionally, attempting to deliver the data file comprises delivering the data file in a unicast transmission to each of the determined receivers. Optionally, attempting to deliver the data file comprises delivering the data file in a multicast transmission to a plurality of the determined receivers.

Optionally, attempting to deliver the data file comprises providing a notification message inviting the receivers to download the transmission on a unicast connection, to the determined receivers. Optionally, at least 80% of the designated receivers establish only a single unicast connection related to receiving the data file. Optionally, substantially all of the designated receivers establish only a single unicast connection related to receiving the data file. Optionally, substantially all of the designated receivers establish up to two single unicast connections related to receiving the data file. Optionally, at least a portion of the data file is encrypted, requiring one or more decryption keys identified in the transmitted data file.

Optionally, the receivers request the one or more keys after receiving the data file. Optionally, the receivers request the one or more keys after determining that they received sufficient data to allow reconstruction of the data file. Optionally, the keys are received on a single unicast connection along with any supplementary data required, not received during the multicast transmission. Optionally, the method includes receiving acknowledgements from receivers that received the notification or at least a portion of the data file, after transmitting the data file, wherein determining receivers designated that did not receive at least a portion of the data file is performed by determining receivers from which acknowledgments were not received.

Optionally, receiving the acknowledgements comprises receiving a request for decryption keys. Optionally, receiving the acknowledgements comprises receiving a request for supplementary data not received during the multicast transmission. Optionally, receiving the acknowledgements comprises receiving over a different network than the network on which the data file was multicast. Optionally, the data file includes a non-encrypted preview portion. Optionally, the non-encrypted preview portion is transmitted on the multicast channel interleaved with the remaining portion of the data file. Optionally, at least one occurrence of the non-encrypted preview portion is transmitted on the multicast channel before transmission of the remaining portion of the data file.

Optionally, tuning onto the multicast channel comprises tuning onto a cellular multicast channel. Optionally, tuning onto the multicast channel comprises tuning onto a digital video broadcast channel. Optionally, attempting to deliver the data file to the determined receivers comprises delivering on a different network than the network on which the data file was multicast. Optionally, the notification indicates a plurality of categories to which the data file relates and the plurality of receivers comprises receivers designated to receive data belonging to different ones of the plurality of categories.

There is further provided in accordance with an exemplary embodiment of the invention, a method of receiving a data file provided in a multicast transmission, comprising tuning, by a mobile station, onto a multicast channel, receiving at least one encrypted packet which can be used in reconstructing the data file, on the multicast channel and receiving at least one key required for decrypting the at least one packet after receiving the packet.

Optionally, receiving the at least one encrypted packet comprises receiving a plurality of encrypted packets. Optionally, the plurality of encrypted packets require at least two different keys for decryption. Optionally, the at least one key is received after receiving a sufficient number of packets for reconstructing the data file. Optionally, the method includes requesting the at least one key after receiving a sufficient number of packets for reconstructing the data file and wherein receiving the at least one key is performed responsive to the requesting.

Optionally, the requesting of the at least one key is performed responsive to a user instruction. Optionally, at least a portion of the data file is not encrypted. Optionally, the user instruction is received after displaying the non-encrypted portion of the file to the user.

Optionally, the non-encrypted portion of the file is received before any encrypted portion of the data file. Optionally, the user instruction is received before receiving any encrypted portion of the data file. Optionally, the user instruction is received after receiving at least some of the encrypted packets. Optionally, the file includes a plurality of different portions requiring different keys for decryption. Optionally, the keys required for at least one portion are received after displaying at least one other portion. Optionally, the keys required for at least one portion are received after displaying at least one other portion which was decrypted.

Optionally, tuning onto the multicast channel is performed responsive to receiving a notification on an upcoming multicast transmission and responsive to a determination that the upcoming multicast transmission matches a subscription profile of the receiver. Optionally, the determination that the upcoming multicast transmission matches a subscription profile of the receiver comprises consulting a multicast subscription profile stored on the receiver. Optionally, the determination that the upcoming multicast transmission matches a subscription profile of the receiver comprises consulting a multicast subscription profile stored on the receiver which is configured automatically by instructions from a remote unit. Optionally, the determination that the upcoming multicast transmission matches a subscription profile of the receiver comprises consulting a multicast subscription profile stored on the receiver which is configured by a user of the receiver. Optionally, the method includes acknowledging receipt of the at least one key, in a manner which allows charging for the data file.

There is further provided in accordance with an exemplary embodiment of the invention, a method of transmitting multicast data, comprising estimating one or more transmission parameter values required to achieve, on the average, a reception rate of the multicast data lower than 100%, by the receivers to which the multicast data is directed, transmitting the multicast data on a multicast channel, using the one or more estimated parameter values, and providing at least supplementary portions of the multicast data to receivers that did not receive the multicast data in its entirety on the multicast channel.

Optionally, the one or more transmission parameters comprise a transmission power level and/or a FEC redundancy level. Optionally, estimating the one or more transmission parameter values comprises estimating based on general network data without relation to specific conditions of a current transmission. Optionally, estimating the one or more transmission parameter values comprises estimating based on specific conditions of a current transmission. Optionally, estimating the one or more transmission parameter values comprises estimating based on the number of receivers. Optionally, the multicast channel comprises a data channel of a cellular network.

There is further provided in accordance with an exemplary embodiment of the invention, a method of receiving multicast data in a cellular network, comprising establishing, by a mobile station, a data channel, through a first network unit of a first mobile network, opening, by the mobile station, a port associated with the data channel, and receiving, by the mobile station, through the port, multicast data from a multicast channel passing through a second network element, belonging to a second mobile network different from the first mobile network.

Optionally, establishing the data channel comprises receiving an IP address for the mobile station and/or establishing a packet data context. Optionally, the first and second network elements comprise GGSNs. Optionally, the method includes receiving a key for decrypting the multicast data through the first network element.

There is further provided in accordance with an exemplary embodiment of the invention, a method of transmitting multicast data in a cellular network, comprising providing data for multicast transmission to a plurality of base stations having different bandwidth amounts allocated for multicast transmission, at a same rate, dropping data by one or more of the base stations, as required, so that the data can be transmitted by each of the base stations on its respective allocated bandwidth for multicast transmission and transmitting the non-dropped data such that the data is transmitted by all the base stations substantially synchronously.

Optionally, the base stations use a small buffer for the provided multicast data.

There is further provided in accordance with an exemplary embodiment of the invention, a method of transmitting multicast data in a cellular network, comprising transmitting a notification on an upcoming transmission of a multicast file, stating a plurality of categories to which the data file relates and tuning on to a multicast channel by a plurality of receivers subscribed to different categories, responsive to the notification.

BRIEF DESCRIPTION OF FIGURES

Particular non-limiting embodiments of the invention will be described with reference to the following description of embodiments in conjunction with the figures. Identical structures, elements or parts which appear in more than one figure are preferably labeled with a same or similar number in all the figures in which they appear, in which:

Fig. 1 is a schematic illustration of a cellular network, in accordance with an exemplary embodiment of the present invention;

Fig. 2 is a flowchart of acts performed by network elements in multicasting a file to mobile stations, in accordance with an exemplary embodiment of the invention;

Fig. 3 is a flowchart of acts performed by a mobile station in receiving a multicast data file, in accordance with an exemplary embodiment of the invention; and

Fig. 4 is a schematic illustration of first and second public land mobile networks (PLMNs), useful in explaining cooperation between networks in providing multicast data, in accordance with an exemplary embodiment of the invention.

DETAILED DESCRIPTION OF EMBODIMENTS

Fig. 1 is a schematic illustration of a cellular network 100, in accordance with an exemplary embodiment of the present invention. Network 100 includes a plurality of base stations (BTS) 50, which transmit signals to mobile stations 20 in a cell in their vicinity. Generally, as is known in the art, each group of several base stations 50 are controlled by a base station controller (BSC) 22. As is known in the art, BSC 22 may be replaced by other units, such as by a radio network controller (RNC). Regular unicast data is transmitted to BSC 22 through a serving GPRS support node (SGSN) 24 and a gateway GPRS support node (GGSN) 26 from an IP core network 28, such as the Internet.

In some embodiments of the invention, in transmission of multicast data to mobile stations 20, a data source 30 generates files which are to be multicast to subscribing mobile stations 20. Optionally, the generated files are provided to a data server 42, which controls the provision of the file in a multicast transmission to mobile stations 20.

In some embodiments of the invention, data server 42 includes a forward error correction (FEC) unit 32, in which a plurality of FEC packets are prepared to represent blocks of the file. The FEC packets are generated using substantially any FEC method known in the art, including one-dimensional, two-dimensional, systematic and non-systematic methods. In an exemplary embodiment of the invention, a FEC method such as described in Israel patent application 154,739, filed March 4, 2003 and/or in Israel patent application 157,885, filed September 11, 2003, titled "Iterative Forward Error Correction", the disclosures of which are incorporated herein by reference, is used. The FEC packets are optionally transferred to an encryption unit 34, which encrypts the FEC packets, forming respective encrypted packets. The encryption of the data may be performed using any method known in the art, including symmetric and non-symmetric (i.e., public key and private key) methods. In an exemplary embodiment of the invention, the encryption is performed as described in Israel patent application 157,886, filed September 11, 2003, titled "Secure Multicast Transmission", the disclosure of which is incorporated herein by reference. Optionally, each packet or group of packets is marked with an identification of the key to be used in decoding the packet.

The encrypted packets of each base station 50 are transferred to the base station for transmission in a respective cell covered by the base station. In some embodiments of the invention, for example as shown in Fig. 1, the encrypted packets are provided through a respective point to multipoint unit (PTMU) 40 of the base station. Alternatively, the encrypted packets are provided to the base station along a data channel passing through GGSN 26, SGSN 24 and BSC 22. Optionally, in accordance with this alternative, data server 42 serves as a broadcast multicast service center (BMSC).

In some embodiments of the invention, the multicast data is transmitted by the base stations using the currently available bandwidth not used for other connections. Accordingly, different amounts of bandwidth for multicast may be allocated in different cells. Alternatively or additionally, some or all of the cells allocate a fixed bandwidth for multicast transmission. The fixed bandwidth is optionally determined according to the load in the cell, such that different cells allocate different bandwidth for multicast.

Optionally, the packets are provided to base stations 50 at a same rate in a synchronized manner, so that all the base stations receive the same data at the same time. In some embodiments of the invention, base stations 50 (or the BSCs 22 and/or PTMUs 40 servicing the base stations) whose multicast bandwidth allows a transmission rate lower than the rate at which the data packets are received from data server 42, are configured to drop some of the packets in a manner which keeps close synchronization of the transmitted data between different cells. Thus, a mobile station roaming between cells will not receive a large number of packets twice.

In some embodiments of the invention, the base stations 50 (or any other unit that performs the dropping for the cell) have small buffers (e.g., of the size of 2-5 packets) for the multicast data, so that the time difference between transmitting the same data between different base stations 50 is relatively small. Alternatively or additionally, the data packets are divided into blocks and base stations 50 are configured to drop packets of an old block when a first packet of a new block is received. Further alternatively or additionally, data server 42 transmits periodically an instruction to drop all old packets.

In some embodiments of the invention, identical packets are provided to all the base stations. Alternatively, different packets representing the same data, for example encoded using different keys and/or including different FEC protection segments, are provided to different base stations 50. The transmission of different FEC protection segments in different base stations 50 may be used, in addition to or instead of synchronous transmission, in avoiding reception of duplicate data by a moving mobile station.

Data server 42 optionally includes a key server 36, which provides decryption keys to mobile stations 20. In some embodiments of the invention, mobile stations 20 receiving the file, instructed to display the file, contact key server 36 and request the keys they need for the decryption. In addition, mobile stations 20 that did not receive all the data during the multicast, optionally receive missing data portions from key server 36, acting additionally as a supplementary data server, as described below.

Although data source 30, FEC unit 32, encryption unit 34 and key server 36 are shown as separate units, in some embodiments of the invention, one or more of these units are implemented together. For example, encryption unit 34 and key server 36 may be implemented on a single processor and/or may use a common key database. Alternatively, FEC unit 32, encryption unit 34 and key server 36 may be implemented by a plurality of different units at different locations.

Optionally, key server 36 provides keys for decryption only to mobile stations 20 that have subscribed to the multicast data. Users optionally subscribe for receiving the multicast data with the data content provider. Alternatively or additionally, users register through the cellular service provider. In some embodiments of the invention, data server 42 provides multicast data of a plurality of different categories, for example relating to different themes (e.g., sports, news, music, financial information). Categories may also be based on other attributes, such as profession of the user and/or predefined groups of users. Optionally, key server 36 provides keys for decryption only to mobile stations 20 subscribed to the category to which the transmitted file belongs. Alternatively, for some or all the categories, any user requesting decryption keys is provided the keys and there is no need for prior subscription.

Optionally, some data files may relate to more than one category and are therefore provided to subscribers of all the categories to which they relate. In some embodiments of the invention, different notifications are transmitted for each category to which the data file relates. Alternatively, a single notification stating the categories to which the data file relates is transmitted. For example, each notification may include a list of the category numbers to which it relates. Alternatively, each notification has fields for all the possible categories and a bit is set for each category to which the data file of the notification relates. Each user registering to receive multicast data optionally states the categories the user is interested in.

In some embodiments of the invention, special data files (e.g., an extraordinary news broadcast, a promotion music or video clip) are provided to all subscribers or to all mobile stations, optionally even to those that did not subscribe to any category.

The user is optionally charged a flat price for the subscription to the multicast service and/or for each category the user is subscribed to. Alternatively or additionally, the user is charged for each data file for which decryption keys were requested. In providing the keys, key server 36 optionally marks the identity of the mobile stations 20 requesting keys, for billing purposes. Optionally, data files not delivered within a predetermined time are not billed for, or are provided for a reduced cost. For example, data files provided in a mailbox of the user due to unsuccessful transfer during the multicast, as described below, may be provided at a lower fee. Further alternatively or additionally, the transmission costs of some data files, such as promotion files, are charged to the data provider.

In some embodiments of the invention, data server 42 manages a subscriber list 44 which lists for each of the multicast categories, which mobile stations 20 are subscribed to the data of the group. The subscription information in subscriber list 44 is optionally used in determining whether to provide decryption keys as discussed above. Alternatively or additionally, the information in subscriber list 44 is used in determining that all the subscribed mobile stations 20 received the multicast file, as described hereinbelow. Further alternatively or additionally, the information in subscriber list 44 is used to update mobile stations 20 on the files they should receive, as described hereinbelow.

Fig. 2 is a flowchart of acts performed by network elements in multicasting a file to mobile stations 20, in accordance with an exemplary embodiment of the invention. Data server 42 optionally provides (200) each PTMU 40 with a notification message on an upcoming multicast transmission. Responsive to the notification message, PTMUs 40 generate notification packets which they transmit (202) in their cell. The notification packets optionally include a timing of the transmission and a channel on which the transmission is provided. Alternatively or additionally, the notifications are generated and/or transmitted using any other method known in the art. In an exemplary embodiment of the invention, the notifications are generated automatically responsive to opening a multicast data channel.

At the designated transmission time, optionally without waiting for application layer acknowledgements of the notification messages, the file is transmitted (204) on the multicast channel. After the transmission is completed, and optionally during the transmission, data server 42 waits (230) for unicast connections from MSs 20 receiving the multicast transmission. On the unicast connections, data server 42, for example key server 36 thereof, provides (206) supplementary data and provides (208) decryption keys, as discussed below with reference to Fig. 3. Data server 42 marks (210) mobile stations 20 that requested keys as receiving the data file, for example for billing purposes, as the requesting of the keys serves as an indication that the data file was properly received. That is, mobile stations 20 optionally do not request keys unless they have received sufficient data to reconstruct the file.

After the waiting period, data server 42 optionally determines (232) which mobile stations, subscribed to a multicast group to which the file belongs, did not acknowledge receipt of the data file. These mobile stations 20 may, for example, have been turned off, located in cells not supporting multicast, did not receive the notification message due to data loss and/or did not succeed to establish a unicast connection with key server 36. Optionally, these mobile stations are notified (235) that the data file is waiting for them. The notified mobile stations then optionally establish a unicast connection with key server 36 on which the data file is delivered (237) to the mobile station.

Referring in more detail to transmitting (200) the notification on the upcoming multicast, in some embodiments of the invention the same notification message is provided to each of PTMUs 40 and each PTMU generates a separate notification packet for transmission in its cell. Optionally, the notification message includes a time of beginning of the multicast transmission and/or a duration of the transmission. In an exemplary embodiment of the invention, rather than stating a time for the beginning of the multicast transmission, the multicast transmission is carried out a predetermined time after the notification packet is transmitted. The notification message optionally further includes a file size, information on the type of FEC used and/or the type of encryption used. For each file transmitted, the notification message optionally identifies the multicast category (or categories) to which the file belongs.

The notification packet transmitted by base station 50 is optionally transmitted on a cell broadcast channel. Alternatively or additionally, the notification packet is transmitted as an SMS message to the mobile stations. Further alternatively or additionally, the notification packet is transmitted to the mobile stations using their IP address, for mobile stations having an IP address. In an exemplary embodiment of the invention, in base stations 50 associated with a PTMU 40, the notification packet is generated by the PTMU, while in other base stations the notification packet is provided through a regular cell broadcast service.

In some embodiments of the invention, the notification packet is transmitted to all mobile stations 20 in the network, regardless of whether they are registered to receive the multicast transmission. Optionally, mobile stations 20 not registered to receive the multicast transmission discard the notification in the application layer. Alternatively, the notification is transmitted with a sub-channel identity of the mobile stations registered to the list, such that the mobile stations 20 not on the list discard the notifications in a low communication layer.

Although in the above description each file that is multicast has a separate notification message, in some embodiments of the invention, a single notification message is used for a plurality of files that are multicast. Alternatively or additionally, a plurality of notification messages are generated for a single file, in order to increase the chances that at least one of the notifications will be received. The notification packets optionally have a high FEC protection level, so as to minimize the loss of the notification packet due to an interfering noise.

Referring in more detail to waiting (230) for unicast connections, in some embodiments of the invention, data server 42 optionally waits a predetermined time for acknowledgements after the multicast session is completed. The amount of wait time is optionally selected according to the number of receivers on the list of mobile stations 20 to receive the transmission and/or the transmission rates in the network.

Referring in more detail to notifying (235) the non-acknowledging mobile stations 20 that the file is waiting for them, in some embodiments of the invention, the notification is transmitted on a short message (e.g., SMS). Optionally, the notification is transmitted a plurality of times consecutively in order to reduce the chances that the notification is not received. Alternatively or additionally, the notification is transmitted on a low loss channel and/or with a high forward error protection.

Optionally, before downloading the file, the mobile station verifies that it did not yet receive the file. In some embodiments of the invention, when a relatively large number of mobile stations did not receive the file, the short message indicates an interval in which it is best to download the file (different intervals being indicated to different mobile stations), so as to reduce the load on data server 42.

In some embodiments of the invention, data files delivered (237) on a unicast connection are provided in a different, more efficient, format than provided on the multicast connection (e.g., using less or no FEC protection). Alternatively, for simplicity, the same packets are provided on the unicast connection as on the multicast connection.

In some embodiments of the invention, mobile stations 20 are required to acknowledge receipt of the notification, for example by transmitting a return SMS message. Alternatively, mobile stations 20 do not acknowledge receipt of the notifications and notifications are retransmitted to mobile stations that do not collect the file within a predetermined time.

For mobile stations from which an acknowledgement was not received, repeated attempts are optionally made to provide the notification, until the data is properly delivered. Alternatively, or after a predetermined time (e.g., several hours) and/or a predetermined number of attempts, the data file is considered old and no more attempts to deliver the file are made. Optionally, a message is sent to a mailbox of the mobile station notifying that the old file was not delivered. Optionally, the mobile station 20 can then establish a unicast connection with the data server at any time to collect the old file, if desired. Alternatively or additionally, the old file is placed in a mailbox of the mobile station 20 such that it can be collected therefrom by the user. Optionally, a message reporting the placement of the file in the mailbox is transmitted to the mobile station. In some embodiments of the invention, the reporting message is transmitted only a period of time after the placement in the mailbox, only if the receiver did not pick up the file. Thus, the number of messages required is decreased.

Alternatively to transmitting (235) a notification to the non-acknowledging mobile stations 20, the data file is provided to non-acknowledging mobile stations on a unicast data connection established by key server 36 or on an MMS transmission, with each of the mobile stations. Optionally, in accordance with this alternative, before providing the file on the connection, the mobile station is queried as to whether it has already received the file.

Further alternatively or additionally, data server 42 does not manage a subscription list at all or does not provide the file to mobile stations 20 that do not request the file.

Fig. 3 is a flowchart of acts performed by a mobile station in receiving a file in a multicast transmission, in accordance with an exemplary embodiment of the invention. Upon receiving (250) the notification packet, the mobile station determines (252) whether to receive the file, for example, by consulting a subscription profile record on the mobile station, by determining whether the file was received already and/or by querying the user. If the file is to be received, the mobile station tunes (254) onto the multicast channel on which the file is provided, optionally as identified in the notification packet. The mobile station then receives (256) packets of the file on the multicast channel. During the packet reception, the receiver repeatedly checks (258) if a sufficient group of packets for reconstruction, were received. If (258) a sufficient group of packets for reconstructing the file are received during the multicast session, the mobile station leaves (262) the multicast channel, possibly during the multicast session.

In some embodiments of the invention, the mobile station determines (263) whether to request the keys required for decoding the file. If it is determined to request the keys, the mobile station establishes (264) a unicast connection with key server 36. On the unicast connection, the mobile station 20 requests (266) the keys it requires in order to decode the packets it received, and receives (268) the requested keys on the established unicast connection. The file is then displayed (270) to the user.

If (258) a sufficient number of packets were not received during the multicast session, the mobile station establishes (260) a unicast connection with key server 36 and requests (272) supplementary packets. In some embodiments of the invention, if additional multicast sessions for the same data file are scheduled, the mobile station waits for the additional session and does not request supplementary data yet. Key server 36 provides the supplementary packets on the unicast connection. Thereafter, the mobile station optionally determines (267) whether to request the keys required for decoding the file. If it is determined to request the keys, on the same connection, key server 36 optionally provides (268) the keys required for decrypting the packets. In some embodiments of the invention, mobile station 20 requests the keys after receiving the supplementary packets. Alternatively, mobile station 20 requests the keys along with the request for supplementary packets.

Alternatively, the keys and supplementary data are provided on separate unicast connections. For example, the connections may be established with two separate units, one of which provides the keys and the other provides supplementary data. Alternatively or additionally, the receiver may first receive the entire data file and then ask the user whether to request the keys. For example, as described below, the user may first view a preview of the data before requesting the keys. In some embodiments of the invention, between the two unicast connections, the receiver mobile station 20 does not tune onto the multicast channel for additional data, as the required data is supplemented on the first unicast connection.

In some embodiments of the invention, the received data file includes a non-encoded portion which is previewed by the user in order to determine whether to request the keys of the encoded portion. A data supplementing connection is optionally established, if necessary, before the preview is displayed in order to fill in data required for the preview and a key requesting connection is optionally established after the preview, if desired. Acknowledgement of data receipt may be supplied on either connection. Charging, however, is performed only if keys are requested on the second connection.

In some embodiments of the invention, the data file includes a plurality of portions encoded with different keys. Upon receiving the file, the mobile station requests a first set of keys for decrypting a first portion of the file. Thereafter, based on viewing the first portion of the file, the user instructs mobile station 20 whether to request keys for one or more additional portions of the file. Based on viewing the additional portions, the user may determine whether to request keys for further portions of the file. Optionally, the order of requesting keys is predetermined, such that key server 36 will not provide keys for a second portion if keys for the first portion were not requested. Alternatively, the encrypting is performed in a manner which allows decryption only according to the allowed order. In some embodiments of the invention, according to the allowed decryption order of the portions, each portion is encrypted with a function of all the keys of the previous portions in addition to its key. Thus, each portion can only be decrypted after receiving all the keys of the previous portions. Alternatively, the last portion is encrypted first with its key. Thereafter, the last portion and the previous portion is encrypted with the key of the previous portion. This process is optionally continued for all the portions, so that to decrypt a portion its keys and the keys of all the portions before it are required.

In some embodiments of the invention, the user is notified when receiving the first portion on the structure of the file and the number of portions it has. The user can then request the keys for all the portions at once or request one or more keys in a plurality of separate requests. Alternatively, the user is not notified as to the structure of the file in advance, and each time the user requests keys, the user is provided with a set of keys of the next portion. Further alternatively, the user may determine which of the portions to decode, in substantially any order.

Alternatively to mobile station 20 automatically requesting the keys for the first portion, the keys are requested only after receiving an instruction from the user, for example after viewing a free preview. In some embodiments of the invention, the file includes a plurality of free previews for different encoded portions.

Alternatively to the preview portions being non-encoded, the preview portions are encoded with a special key for previews. The preview key is optionally provided to subscribing mobile stations upon subscription, before the file is transmitted on the mobile channel. Alternatively, the key is requested by the mobile station after the receiving of the data and serves as a first indication of the reception of the data.

Referring in more detail to receiving (250) the notification packet, in some embodiments of the invention, the notification packet includes a low level indication (e.g., a multicast group address) of the mobile stations to which it is directed, and the mobile station provides the notification to the application layer only if the notification packet is directed to the mobile station (e.g., the low level indication matches the mobile station).

Referring in more detail to determining (252) whether to receive the file, in some embodiments of the invention, each mobile station 20 manages a subscription profile which lists the categories to which it is subscribed. Upon receiving the notification packet, the mobile station 20 optionally consults its subscription profile to determine whether to receive the file referred to in the notification packet. Alternatively or additionally, mobile station 20 displays or sounds a message to the user, asking whether to receive the file. Optionally, in accordance with this alternative, mobile station 20 is configured with default decisions on the acts to be performed when a response is not received from the user. For example, a mobile station 20 may be configured to receive all files of a first multicast category, to ask the user about files of a second multicast category but to receive the file if no answer is received and to ask the user about files of a third multicast category but not to receive the file unless specific instructions were received from the user. It is noted that the decision on whether to receive the data of the file is separate from the decision on whether to decode the file and pay for it. A user may decide, for example, to receive any file that has a fair chance to be decoded, in order not to lose time until the file is received, although such reception utilizes the battery power of the mobile station.

In some embodiments of the invention, the rules on whether to receive a file, query the user and/or not receive a file may depend on one or more external parameters not related to the transmission (e.g., the time, date, location of the mobile) and/or one or more internal parameters related to the transmission (e.g., file size, planned transmission rate, expected error rate).

In some embodiments of the invention, the subscription profile in mobile station 20 is configured by the user of mobile station 20, through a user interface of the mobile station, according to user preferences. Alternatively, the subscription profile is configured by a control message transmitted from data server 42 (or from any other remote network unit), according to subscription information in subscription list 44. The control messages are optionally transmitted to mobile station 20 periodically and/or whenever there is a change in the subscription information.

Alternatively to mobile station 20 keeping track of the categories of files it is to receive, the notification packets are transmitted only to mobile stations 20 that are to receive the message, for example using directed unicast SMS messages. Alternatively or additionally, upon receiving the notification packet, mobile stations 20 that do not know if they are to receive the file, query data server 42.

In some embodiments of the invention, a mobile station 20 that received the notification but will not be receiving the file, although being subscribed to receive the file according to subscription list 44, notifies data server 42, so that attempts will not be made to deliver the packet to the mobile station on a unicast connection. Alternatively, the mobile station does not notify data server 42. Optionally, in this alternative, the mobile station ignores the message notifying that the file can be retrieved in unicast or notifies the data server that it is not receiving the file upon receiving the message.

In some embodiments of the invention, the same file is transmitted on the multicast channel a plurality of times in order to make sure that as many as possible receivers receive the file in a multicast transmission. For example, if after a first multicast session of transmitting the file, less than a predetermined number (70-80%) of subscribers acknowledge receipt, instead of providing the file in unicast to all the other subscribers, the file is retransmitted in another unicast session. Alternatively or additionally, a second multicast session is used without relation to the number of acknowledgments received, to make sure that as many as possible receivers use the multicast session to receive the file. The number of multicast sessions is optionally adjusted according to the number of subscribed mobile stations that did not acknowledge reception yet. Optionally, repeated multicast sessions are conducted until the number of non-acknowledging subscribers is below a predetermined percentage.

The multicast sessions may be conducted substantially immediately one after the other, or may be conducted, at different times of the day, e.g., separated by an hour or two. In some embodiments of the invention, each multicast session is preceded by a notification to all the subscribers or to all subscribers that did not acknowledge receipt of the file. Delivery of the file to non-acknowledging mobile stations is optionally performed after all the multicast sessions were completed. Optionally, in these embodiments, in determining (252) whether to receive the file, mobile station 20 verifies that the file was not yet received.

Referring in more detail to tuning (254) to the multicast channel, in some embodiments of the invention, the tuning (254) to the multicast channel is performed passively by mobile station 20, without exchanging link layer packets with the network. Alternatively, before tuning onto the channel, mobile station 20 transmits a link layer message to PTMU 40, notifying that the mobile station is interested in receiving the multicast file. A PTMU 40 that did not receive responses from any mobile stations 20, optionally does not transmit the multicast data. Alternatively or additionally, the link layer responses are used by PTMU 40 to determine the layout of the mobile stations 20 interested in the multicast file in its cell. In some embodiments of the invention, PTMU 40 determines according to the received link layer responses, whether to transmit the data in multicast or in unicast or in a combination thereof. Optionally, a cost function is calculated for multicast transmission and for unicast transmission and the cheaper alternative is used. In some embodiments of the invention, the multicast transmission is given an extra preference score for the possibility that mobile stations currently in other cells will enter the cell of the PTMU 40 during the multicast transmission.

In some embodiments of the invention, the link layer responses and/or the determined mobile station layout of the cell are used in selecting parameters of the transmission, such as the power level of the transmission, the frame error protection and/or any other parameter affecting the average energy per bit of the transmission.

The parameters are optionally selected so as to ensure proper reception of the file by a percentage of the mobile stations lower than 100%, for example between 90-95%. Generally, ensuring proper reception of the file by 100% of mobile stations 20 in the cell requires a relatively large amount of resources, higher than required for achieving reception by 90-95% of the mobile stations and supplementing the rest in unicast.

Alternatively or additionally, one or more transmission parameters are selected by data server 42, so as to achieve a desired percentage of successfully receiving mobile stations 20. Optionally, the transmission parameters are automatically selected according to periodic updates on the state of the network, not received responsive to the current transmission. Alternatively or additionally, the transmission parameters are configured by a network operator according to the general structure of the network and/or the desired service characteristics. The transmission parameters controlled by data server 42 optionally include the level of redundancy of the FEC, the transmission rate and/or the number of retransmissions of the data. The selection of transmission parameters is optionally performed responsive to the average number of receivers, the size of the transmitted file and the network loss rate.

Optionally, before tuning onto the multicast channel, mobile station 20 requests an IP address to be used in receiving the data. The same IP address is optionally used for the unicast connection.

Alternatively or additionally to determining (267) whether to request the keys required for decoding the file after the supplementary data is received, in some embodiments of the invention, the determination is performed before requesting (272) the supplementary data or before establishing (260) the unicast connection, such that the supplementary data is not requested unless the keys will be requested.

Referring in more detail to establishing (260 or 264) the unicast connection, in some embodiments of the invention, mobile stations 20 determine when to request the keys at least partially randomly, so that the load on key server 36 is distributed over the waiting period. Alternatively or additionally, mobile stations 20 receiving all the data during the multicast session may contact key server 36 immediately, while mobile stations 20 requiring supplementary data contact key server 36 at a random interval after the multicast session.

Alternatively or additionally, different base stations 50 instruct the mobile stations they service, for example in the notification packets, on different times at which they are to contact key server 36. Alternatively or additionally, a plurality of key servers are provided and the notification packets instruct the mobile stations 20 as to which key server they are to contact.

In some embodiments of the invention, the multicast data may be received even by mobile stations 20 that do not have an IP address. Optionally, if the mobile station does not already have an IP address, establishing the unicast connection includes requesting an IP address from GGSN 26. In some embodiments of the invention, the unicast connection is established through a wireless application protocol (WAP) gateway. Optionally, in some of these embodiments, the entire provision of the data file, including the requesting of supplementary data and decryption keys is performed without the mobile station having an IP address.

Referring in more detail to determining (263 or 267) whether to request the keys, in some embodiments of the invention, the user decides whether to request the keys. Optionally, the decision is made based on viewing the preview. Alternatively or additionally to the user deciding whether to request the keys, the user and/or a system operator may configure the mobile station with rules on when to request the keys automatically. The rules on when to request the keys automatically may optionally be the same as the rules for receiving the file and/or may be different from the rules for receiving the data. Optionally, the preview portion of the file includes information which can be used in automatically determining whether to request the keys. For example, in providing sport clips, the data may include the teams involved or the time during the game. A user may configure his/her mobile to automatically request keys for games of a certain team and/or occurring at a specific time during the game.

Referring in more detail to providing supplementary packets in response to requesting (272) supplementary data, optionally, the mobile station determines a minimal set of packets required in order to allow reconstruction of the data file and requests these specific packets. Alternatively, the mobile station notifies server 38 which packets it received and the data server determines a minimal set of packets to be provided to the mobile station. Further alternatively, the supplementary packets include original packets, even if requiring transmission of a larger number of packets than optimal. Further alternatively or additionally, during the unicast connection mobile station 20 periodically determines whether it has sufficient packets for reconstruction and accordingly requests more packets.

The supplementary packets and/or data files provided on unicast connections are optionally provided along with the keys required for decoding the data. Alternatively, the supplementary packets and/or the data files provided on unicast connections are provided non-encoded. Further alternatively, as with multicast data, the mobile station must request the keys separately, even if on the same connection, as a verification that the data was properly received.

In some embodiments of the invention, users receiving some of the multicast files are encouraged to transfer the files to their friends using a unicast transmission service, such as

MMS. The cellular service provider receives revenues from such transmission. In addition, such transfer could induce users to subscribe. Alternatively or additionally, some multicast files are prevented from being distributed to non-subscribers, for example using digital right management (DRM) methods to limit distribution.

In some networks, in order for a mobile station 20 to transmit data on an application layer uplink, or even a network or transport layer link, the mobile station needs to leave the multicast connection and establish a unicast connection. In order to continue receiving the multicast data, the mobile station would need to retune onto the multicast channel. The changing of channels is generally time consuming and therefore reduces the transmission quality. In the above described embodiments, each mobile station 20 is required to transmit messages to contact data server 42 only a limited number of times, for receiving the multicast file, thus simplifying the network operation in providing multicast data.

In some embodiments of the invention, each mobile station establishes only a single application layer unicast connection in order to receive the multicast data, from the receiving of the notification to the reconstructing of the file. Optionally, beyond the single application layer connection, the mobile stations do not establish any transport or network layer connections in connection with receiving the data file. Alternatively to receiving the data on an application layer connection, the data may be received using a transport layer connection or even a network layer connection without using an application layer.

The uplink transmissions are optionally carried out after the multicast transmission, such that there is no need to re-tune onto the multicast channel.

Uplink application layer transmissions, as well as transport and network layer transmissions, generally differ from link layer transmissions in that link layer transmissions do not require establishing a connection. In addition, the application layer transmissions are generally directed to units out of the public land mobile network (PLMN) servicing the mobile station, while link layer transmissions are directed to elements of the PLMN. The application layer transmissions of substantially all the mobile stations are generally handled by a single server or by a plurality of synchronized servers. Link layer transmissions, on the other hand, are generally handled by respective local network units which are not synchronized regarding the data exchanged with the mobile stations.

In the above exemplary embodiment, the application layer uplink transmissions are for requesting supplementary data, requesting decoding keys and/or reception acknowledgement.

Alternatively to receiving the entire file before previewing and deciding whether to receive the file and/or request the decoding keys, in some embodiments of the invention, the preview may be viewed before receiving all the data. Optionally, during the multicast transmission, the preview can be reconstructed separately from the encoded data, e.g., there are separate FEC blocks for the preview. When a receiver determines that it has a sufficient number of packets for preview, the receiver optionally reconstructs and displays the preview immediately. Thus, the user can decide that the file is not desired even before receiving the entire file, so that battery power can be conserved.

Further alternatively or additionally, the notification packet indicates a series of transmission sessions. In an exemplary embodiment of the invention, the series of transmission sessions includes a preview transmission session and a data file transmission session. Optionally, the preview session is carried out a few minutes before the data transmission, so that the user has sufficient time to decide whether to receive the file before the file multicast session begins. Optionally, acknowledgements are transmitted only after the data transmission sessions. In some embodiments of the invention, users that are sure they want to receive the data file can configure their mobile station to forego receiving the preview.

In some embodiments of the invention, mobile stations 20 that need supplementary packets for the preview contact data server 42 and receive the data packets on a unicast connection. Alternatively, supplementary packets for the preview are transmitted during the file multicast session. In this alternative, mobile stations that did not receive a sufficient number of packets during the preview session, and therefore could not view the preview, begin receiving the file during the file multicast session, in case the user will decide to receive the file when the preview is viewed. If the preview is reconstructed during the file multicast session and the user decides not to receive the file, the mobile station is instructed to stop receiving the file. Optionally, the user configures the mobile station as to whether it waits for viewing the preview until the file multicast session or requests supplementary preview packets on a unicast connection. It is noted that in these embodiments mobile stations that request supplementary preview packets and request the keys for the data file will establish two unicast connections in receiving the multicast data file.

Fig. 4 is a schematic illustration of first and second public land mobile networks (PLMNs), useful in explaining cooperation between networks in providing multicast data, in accordance with an exemplary embodiment of the invention. A mobile station 320 registered for service by a PLMN A 302 is currently in a district not serviced by PLMN A, but is serviced by PLMN B 304, which has a cooperation agreement with PLMN A. PLMN B 304 delivers multicast data to subscribing users, for example using methods described above. The delivered multicast data is optionally encrypted and users pay for the decryption keys.

Generally, as is known in the art, when mobile station 320 enters the area covered by PLMN B 304, the mobile station registers with PLMN B such that it exchanges periodic servicing signals with a BSC 310 of PLMN B or with other control units of PLMN B. PLMN B notifies PLMN A that mobile station 320 is serviced by PLMN B. Unicast data connections initiated by mobile station 320 are generally tunneled to PLMN A 302 which services the data connections. Telephone calls directed to mobile station 320 are received by PLMN A which forwards the calls to PLMN B. Telephone calls generated by mobile station 320 are generally directed through PLMN B.

In some embodiments of the invention, when PLMN B provides a multicast file, mobile station 320 receives the notification packet on the upcoming multicast and determines whether to receive the multicast file. The decision is optionally performed without communicating with PLMN B at all or using only link layer communication with PLMN B. If mobile station 320 is instructed by the user to receive the file, the mobile station tunes onto the multicast channel and receives the packets of the file. The multicast data is provided from a data server 344 of PLMN B through BSC 310. Optionally, PLMN B does not know whether mobile station 320 received the multicast data and therefore cannot, for example, generate a charge data record (CDR) for the mobile station 320.

Thereafter, mobile station 320 contacts a data server 342 of PLMN A to request supplementary data, if necessary, and deciphering keys. The contact with data server 342 is optionally performed through an SGSN 333 of PLMN B and a GGSN 337 of PLMN A. Data server 342 of PLMN A requests the keys and supplementary data from data server 344 of PLMN B and provides the keys back to mobile station 320. If unicast delivery is required, e.g., mobile station 320 is subscribed to receive the file but did not receive the notification, the unicast delivery is performed by data server 342 of PLMN A. Optionally, a data server of PLMN A authorizes and charges mobile station 320 for the data file.

Alternatively to providing the multicast data in a different cellular network, the multicast data may be provided on a totally different type of network, such as on a terrestrial network (e.g., a digital video broadcast terrestrial (DVB-T) network), or a satellite broadcast channel (e.g., a digital video broadcast satellite (DVB-S) network or any other digital broadcast satellite (DBS) network). Further alternatively, the multicast data is provided in a cellular network, while the supplementary data and/or keys are provided in a different type of network, for example on a wireless local area network (WLAN). In some embodiments of the invention, the acknowledgement, keys and/or supplementary data may be provided on a plurality of networks. Optionally, the receiver attempts to respond on the network with the most local coverage, e.g., a wireless LAN network. If the transmission on the most local network is not successful, the receiver attempts to respond on a network with a greater coverage, e.g., a cellular network. If the transmission on the cellular network is not successful, an attempt to respond is made on a terrestrial or satellite network, for example on a satellite uplink ALOHA channel.

In some embodiments of the invention, PLMN A provides the same multicast data at substantially the same time as the data is provided by PLMN B. In this embodiment, PLMN A does not need to contact PLMN B for supplementary data. PLMN A may, however, need to request the encryption keys from PLMN B. Alternatively, PLMN A does not provide the data at the same time as PLMN B. Optionally, PLMN B provides supplementary data upon request from PLMN A. Alternatively, for example when many supplementary data requests are expected, PLMN B provides all the data to PLMN A in parallel to transmitting the multicast data. In some embodiments of the invention, supplementary data received by PLMN A is cached for further use for a predetermined time in which additional requests may be received.

In some embodiments of the invention, contacting data server 342 of PLMN A by mobile station 320 includes establishing a data channel. Establishing the data channel optionally includes receiving an IP address and/or a packet data context. The packet data context optionally includes setting a QoS for the data channel.

In some embodiments of the invention, each PLMN advertises a unique ID of the PLMN in the control signals it transmits. Different PLMNs optionally communicate with each other through gateways that are used for security.

It will be appreciated that the above described methods may be varied in many ways, including, changing the order of steps, and the exact implementation used. The methods of the present invention may be performed in various protocol layers and may be performed for a single transmission system in a plurality of communication protocol layers. It should also be appreciated that the above described methods and apparatus are to be interpreted as including apparatus for carrying out the methods and methods of using the apparatus.

The present invention has been described using non-limiting detailed descriptions of embodiments thereof that are provided by way of example and are not intended to limit the scope of the invention. For example, in some embodiments of the invention, mobile stations are required to acknowledge the notification packet and unicast notifications are transmitted to non-acknowledging mobile stations.

It should be understood that features and/or steps described with respect to one embodiment may be used with other embodiments and that not all embodiments of the invention have all of the features and/or steps shown in a particular figure or described with respect to one of the embodiments. Variations of embodiments described will occur to persons of the art.

It is noted that some of the above described embodiments may describe the best mode contemplated by the inventors and therefore may include structure, acts or details of structures and acts that may not be essential to the invention and which are described as examples. Structure and acts described herein are replaceable by equivalents which perform the same function, even if the structure or acts are different, as known in the art. Therefore, the scope of the invention is limited only by the elements and limitations as used in the claims. When used in the following claims, the terms "comprise", "include", "have" and their conjugates mean "including but not limited to".

CLAIMS

1. A method of multicasting a data file, comprising:

transmitting a notification on an upcoming multicast transmission to a plurality of receivers designated to receive the multicast transmission;

tuning by at least one of the plurality of receivers to a multicast channel, responsive to the notification;

transmitting a data file, from a data server, on the multicast channel, without the data server receiving acknowledgements from the receivers on whether they received the notification;

determining receivers designated to receive the multicast transmission that did not receive at least a portion of the data file; and

attempting to deliver the data file to the determined receivers.

2. A method according to claim 1, wherein transmitting the notification comprises transmitting on a multicast or broadcast channel.

3. A method according to claim 1, wherein transmitting the notification comprises transmitting a unicast notification to each of the receivers on the designated receivers.

4. A method according to any of the preceding claims, wherein transmitting the notification comprises transmitting substantially only to designated receivers.

5. A method according to any of the preceding claims, wherein transmitting the notification comprises transmitting a message open also to non-designated receivers.

6. A method according to any of the preceding claims, wherein the notification indicates the channel on which the multicast transmission will be provided.

7. A method according to any of the preceding claims, wherein tuning to the multicast channel by at least one of the receivers comprises determining by each receiver that receives the notification whether to tune onto the multicast channel.

8. A method according to claim 7, wherein determining by each receiver that receives the notification whether to tune onto the multicast channel comprises determining, from the notification, a group to which the upcoming multicast transmission belongs and determining whether to tune to the multicast channel according to the determined group.

9. A method according to claim 7 or claim 8, wherein determining by each receiver that receives the notification whether to tune onto the multicast channel comprises determining by consulting a list stored on the receiver.

10. A method according to any of claims 7-9, wherein determining by each receiver that receives the notification whether to tune onto the multicast channel comprises determining based on input received from a user responsive to the notification.

11. A method according to any of the preceding claims, wherein the receivers do not transmit acknowledgements of reception of the notification, at all.

12. A method according to any of the preceding claims, wherein the receivers cannot transmit uplink messages to the data server, without stopping to listen to the multicast channel.

13. A method according to any of the preceding claims, wherein attempting to deliver the data file comprises delivering the data file in a unicast transmission to each of the determined receivers.

14. A method according to any of claims 1-12, wherein attempting to deliver the data file comprises delivering the data file in a multicast transmission to a plurality of the determined receivers.

15. A method according to any of the preceding claims, wherein attempting to deliver the data file comprises providing a notification message inviting the receivers to download the transmission on a unicast connection, to the determined receivers.

16. A method according to any of the preceding claims, wherein at least 80% of the designated receivers establish only a single unicast connection related to receiving the data file.

17. A method according to claim 16, wherein substantially all of the designated receivers establish only a single unicast connection related to receiving the data file.

18. A method according to claim 16 or claim 17, wherein substantially all of the designated receivers establish up to two single unicast connections related to receiving the data file.

19. A method according to any of the preceding claims, wherein at least a portion of the data file is encrypted, requiring one or more decryption keys identified in the transmitted data file.

20. A method according to claim 19, wherein the receivers request the one or more keys after receiving the data file.

21. A method according to claim 19 or claim 20, wherein the receivers request the one or more keys after determining that they received sufficient data to allow reconstruction of the data file.

22. A method according to claim 19, wherein the keys are received on a single unicast connection along with any supplementary data required, not received during the multicast transmission.

23. A method according to any of the preceding claims, comprising receiving acknowledgements from receivers that received the notification or at least a portion of the data file, after transmitting the data file, wherein determining receivers designated that did not receive at least a portion of the data file is performed by determining receivers from which acknowledgments were not received.

24. A method according to claim 23, wherein receiving the acknowledgements comprises receiving a request for decryption keys.

25. A method according to claim 23 or claim 24, wherein receiving the acknowledgements comprises receiving a request for supplementary data not received during the multicast transmission.

26. A method according to any of claims 23-25, wherein receiving the acknowledgements comprises receiving over a different network than the network on which the data file was multicast.

27. A method according to any of the preceding claims, wherein the data file includes a non-encrypted preview portion.

28. A method according to claim 27, wherein the non-encrypted preview portion is transmitted on the multicast channel interleaved with the remaining portion of the data file.

29. A method according to claim 27, wherein at least one occurrence of the non-encrypted preview portion is transmitted on the multicast channel before transmission of the remaining portion of the data file.

30. A method according to any of the preceding claims, wherein tuning onto the multicast channel comprises tuning onto a cellular multicast channel.

31. A method according to any of the preceding claims, wherein tuning onto the multicast channel comprises tuning onto a digital video broadcast channel.

32. A method according to any of the preceding claims, wherein attempting to deliver the data file to the determined receivers comprises delivering on a different network than the network on which the data file was multicast.

33. A method according to any of the preceding claims, wherein the notification indicates a plurality of categories to which the data file relates and the plurality of receivers comprises receivers designated to receive data belonging to different ones of the plurality of categories.

34. A method of receiving a data file provided in a multicast transmission, comprising:

tuning, by a mobile station, onto a multicast channel;

receiving at least one encrypted packet which can be used in reconstructing the data file, on the multicast channel; and

receiving at least one key required for decrypting the at least one packet after receiving the packet.

35. A method according to claim 34, wherein receiving the at least one encrypted packet comprises receiving a plurality of encrypted packets.

36. A method according to claim 35, wherein the plurality of encrypted packets require at least two different keys for decryption.

37. A method according to any of claims 34-36, wherein the at least one key is received after receiving a sufficient number of packets for reconstructing the data file.

38. A method according to claim 34, comprising requesting the at least one key after receiving a sufficient number of packets for reconstructing the data file and wherein receiving the at least one key is performed responsive to the requesting.

39. A method according to claim 34, wherein the requesting of the at least one key is performed responsive to a user instruction.

40. A method according to claim 39, wherein at least a portion of the data file is not encrypted.

41. A method according to claim 40, wherein the user instruction is received after displaying the non-encrypted portion of the file to the user.

42. A method according to claim 41, wherein the non-encrypted portion of the file is received before any encrypted portion of the data file.

43. A method according to claim 42, wherein the user instruction is received before receiving any encrypted portion of the data file.

44. A method according to claim 42, wherein the user instruction is received after receiving at least some of the encrypted packets.

45. A method according to claim 34, wherein the file includes a plurality of different portions requiring different keys for decryption.

46. A method according to claim 45, wherein the keys required for at least one portion are received after displaying at least one other portion.

47. A method according to claim 46, wherein the keys required for at least one portion are received after displaying at least one other portion which was decrypted.

48. A method according to claim 34, wherein tuning onto the multicast channel is performed responsive to receiving a notification on an upcoming multicast transmission and responsive to a determination that the upcoming multicast transmission matches a subscription profile of the receiver.

49. A method according to claim 48, wherein the determination that the upcoming multicast transmission matches a subscription profile of the receiver comprises consulting a multicast subscription profile stored on the receiver.

50. A method according to claim 49, wherein the multicast subscription profile stored on the receiver is configured automatically by instructions from a remote unit.

51. A method according to claim 49, wherein the multicast subscription profile stored on the receiver is configured by a user of the receiver.

52. A method according to claim 34, comprising acknowledging receipt of the at least one key, in a manner which allows charging for the data file.

53. A method of transmitting multicast data, comprising:

estimating one or more transmission parameter values required to achieve, on the average, a reception rate of the multicast data lower than 100%, by the receivers to which the multicast data is directed;

transmitting the multicast data on a multicast channel, using the one or more estimated parameter values; and

providing at least supplementary portions of the multicast data to receivers that did not receive the multicast data in its entirety on the multicast channel.

54. A method according to claim 53, wherein the one or more transmission parameters comprise a transmission power level.

55. A method according to claim 53 or claim 54, wherein the one or more transmission parameters comprise a FEC redundancy level.

56. A method according to claim 53, wherein estimating the one or more transmission parameter values comprises estimating based on general network data without relation to specific conditions of a current transmission.

57. A method according to claim 53, wherein estimating the one or more transmission parameter values comprises estimating based on specific conditions of a current transmission.

58. A method according to claim 57, wherein estimating the one or more transmission parameter values comprises estimating based on the number of receivers.

59. A method according to claim 53, wherein the multicast channel comprises a data channel of a cellular network.

60. A method of receiving multicast data in a cellular network, comprising:

establishing, by a mobile station, a data channel, through a first network unit of a first mobile network;

opening, by the mobile station, a port associated with the data channel; and receiving, by the mobile station, through the port, multicast data from a multicast channel passing through a second network element, belonging to a second mobile network different from the first mobile network.

61. A method according to claim 60, wherein establishing the data channel comprises receiving an IP address for the mobile station.

62. A method according to claim 60, wherein establishing the data channel comprises establishing a packet data context.

63. A method according to claim 60, wherein the first and second network elements comprise GGSNs.

64. A method according to claim 60, comprising receiving a key for decrypting the multicast data through the first network element.

65. A method of transmitting multicast data in a cellular network, comprising:

providing data for multicast transmission to a plurality of base stations having different bandwidth amounts allocated for multicast transmission, at a same rate;

dropping data by one or more of the base stations, as required, so that the data can be transmitted by each of the base stations on its respective allocated bandwidth for multicast transmission; and

transmitting the non-dropped data such that the data is transmitted by all the base stations substantially synchronously.

66. A method according to claim 65, wherein the base stations use a small buffer for the provided multicast data.

67. A method of transmitting multicast data in a cellular network, comprising:

transmitting a notification on an upcoming transmission of a multicast file, stating a plurality of categories to which the data file relates; and

tuning on to a multicast channel by a plurality of receivers subscribed to different categories, responsive to the notification.

For the applicant,

Fenster & Co. Intellectual Property 2002, Ltd.
c:279/03432

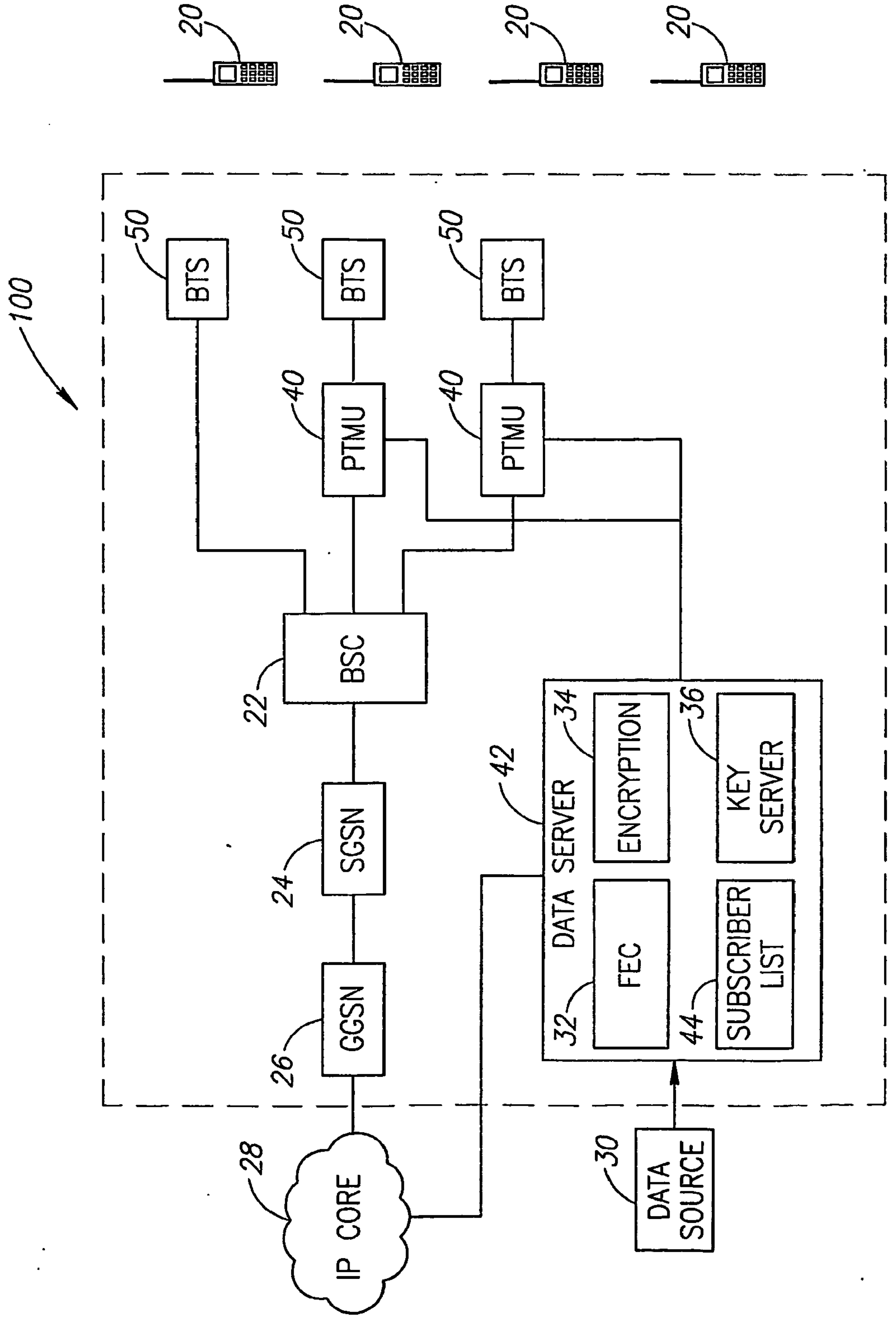
100
20
20
20
20
50
BTS
50
BTS
50
BTS
40
PTMU
40
PTMU
22
BSC
24
SGSN
26
GGSN
28
IP CORE
42
DATA SERVER
32
FEC
34
ENCRYPTION
36
KEY SERVER
44
SUBSCRIBER LIST
30
DATA SOURCE

FIG.1

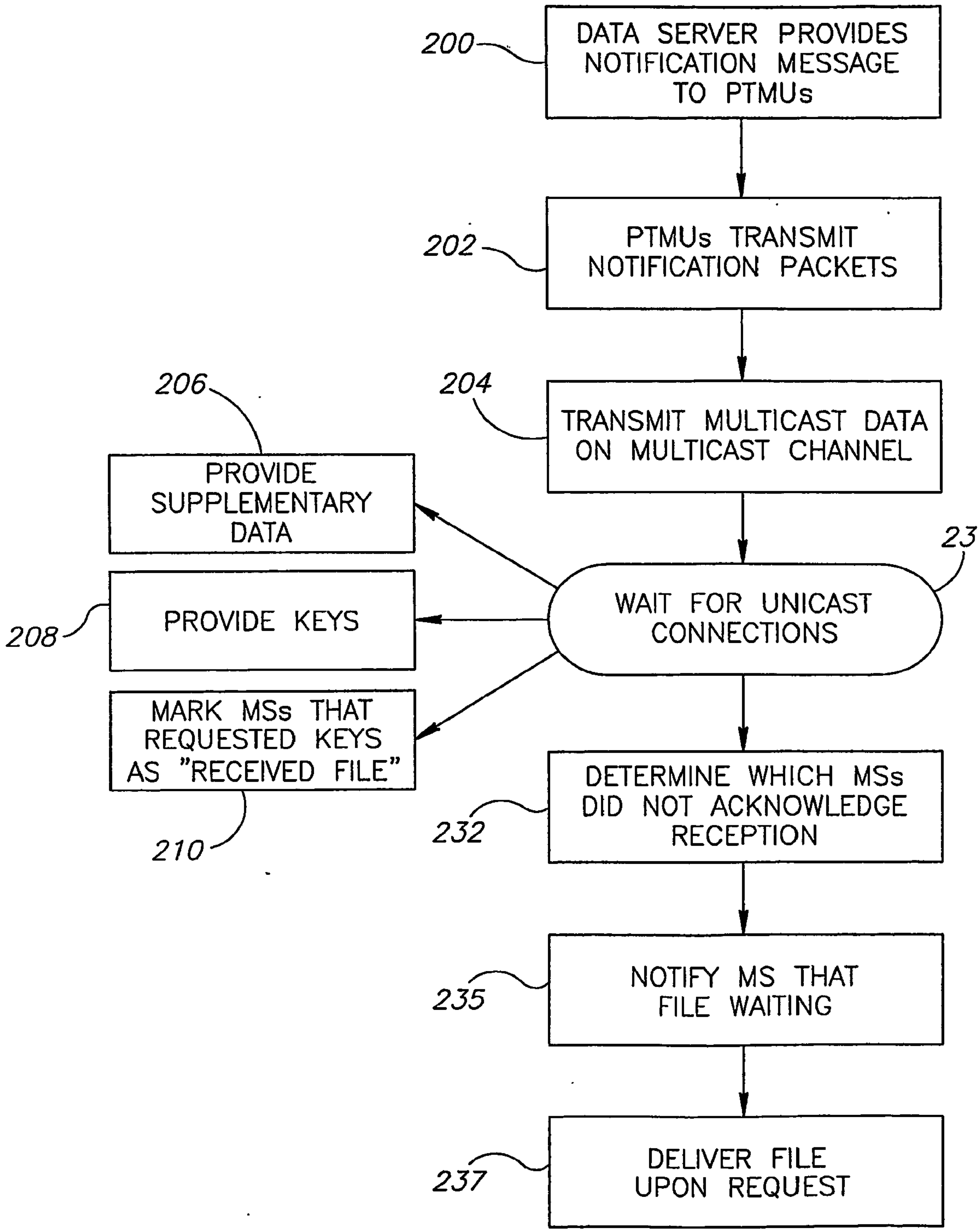
200
DATA SERVER PROVIDES NOTIFICATION MESSAGE TO PTMUs
202
PTMUs TRANSMIT NOTIFICATION PACKETS
204
TRANSMIT MULTICAST DATA ON MULTICAST CHANNEL
230
WAIT FOR UNICAST CONNECTIONS
206
PROVIDE SUPPLEMENTARY DATA
208
PROVIDE KEYS
MARK MSs THAT REQUESTED KEYS AS "RECEIVED FILE"
210
232
DETERMINE WHICH MSs DID NOT ACKNOWLEDGE RECEPTION
235
NOTIFY MS THAT FILE WAITING
237
DELIVER FILE UPON REQUEST

FIG.2

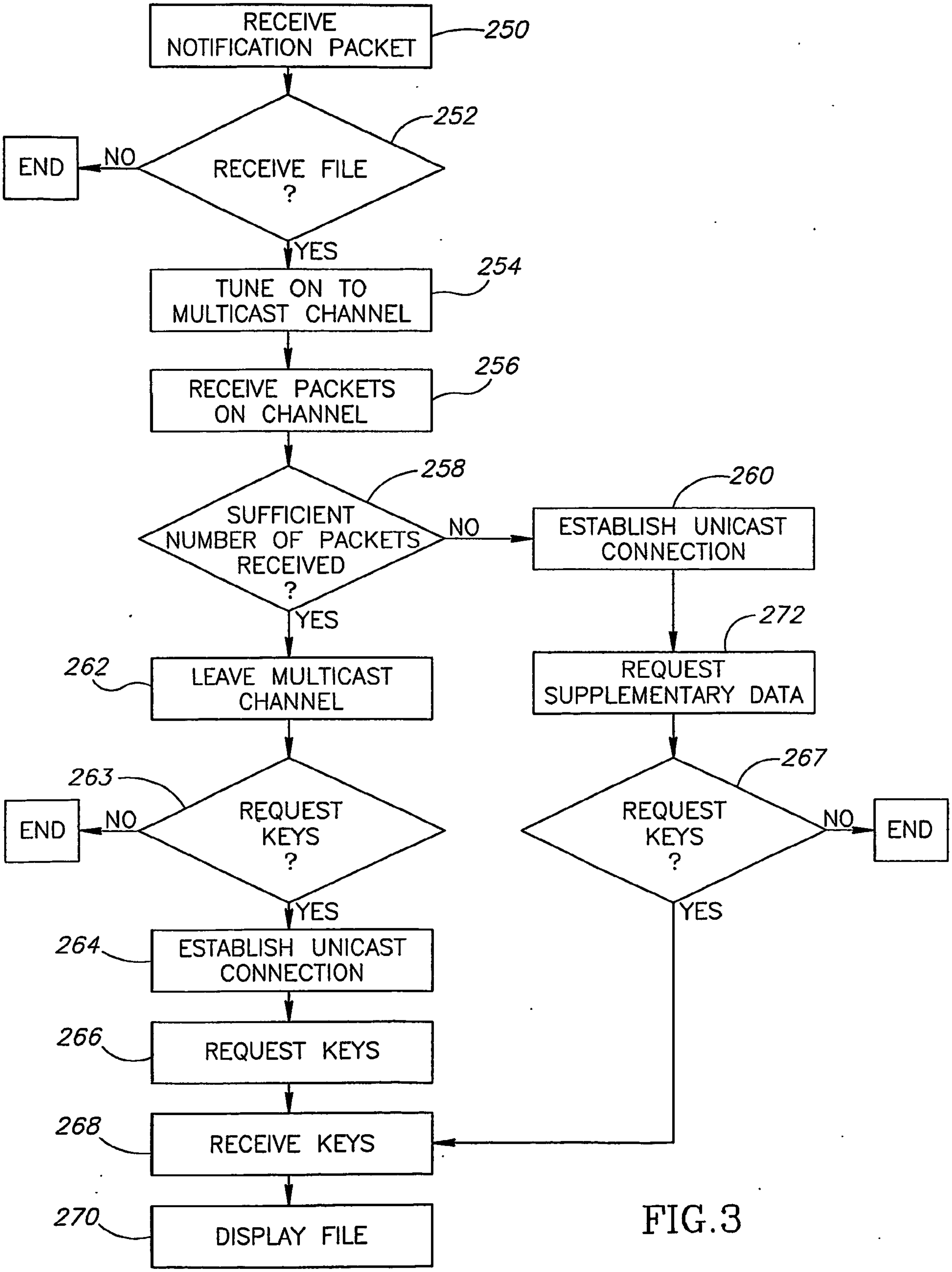
RECEIVE NOTIFICATION PACKET
250
RECEIVE FILE ?
252
NO
END
YES
TUNE ON TO MULTICAST CHANNEL
254
RECEIVE PACKETS ON CHANNEL
256
SUFFICIENT NUMBER OF PACKETS RECEIVED ?
258
NO
ESTABLISH UNICAST CONNECTION
260
YES
LEAVE MULTICAST CHANNEL
262
REQUEST SUPPLEMENTARY DATA
272
REQUEST KEYS ?
263
NO
END
YES
REQUEST KEYS ?
267
NO
END
YES
ESTABLISH UNICAST CONNECTION
264
REQUEST KEYS
266
RECEIVE KEYS
268
DISPLAY FILE
270

FIG.3

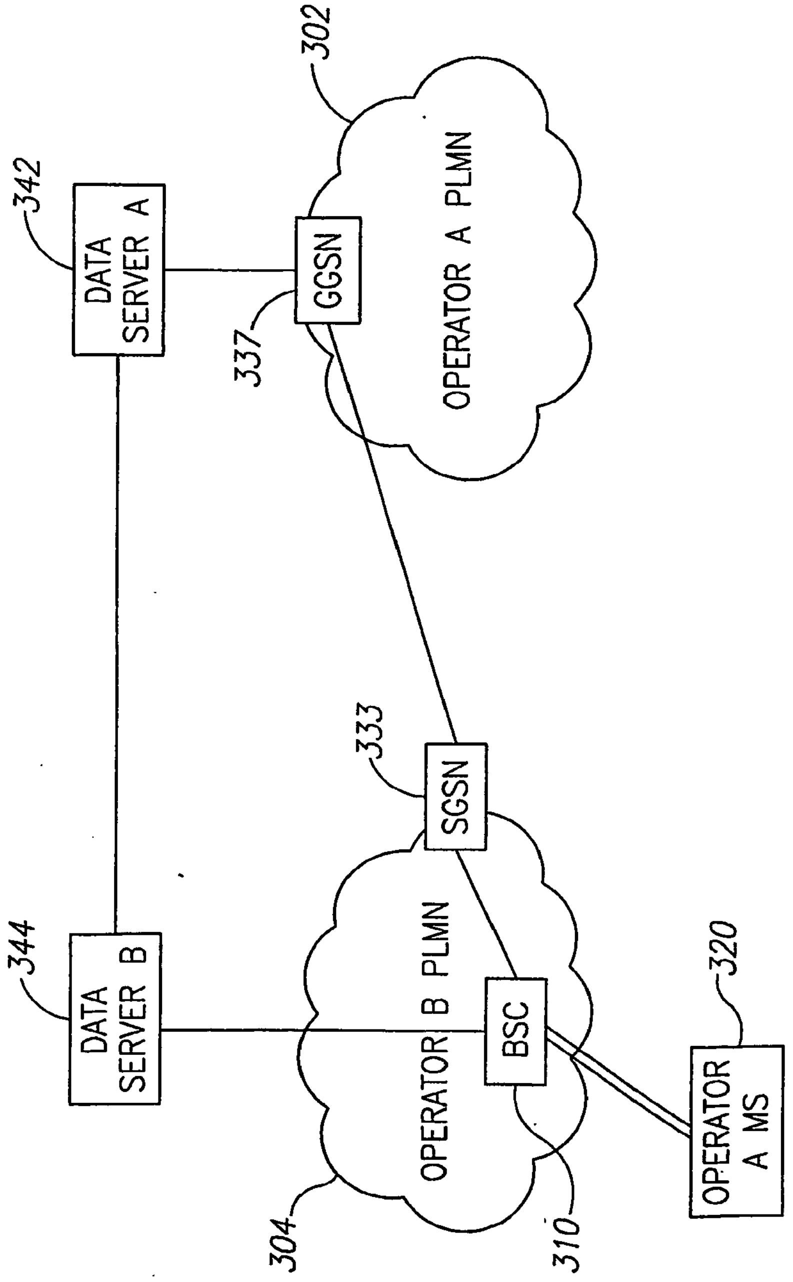
DATA SERVER A
342
GGSN
337
OPERATOR A PLMN
302
SGSN
333
DATA SERVER B
344
BSC
OPERATOR B PLMN
304
310
OPERATOR A MS
320

FIG.4

PCT/IL04/000903

iL04/00903

מדינת ישראל
STATE OF ISRAEL

Ministry of Justice
Patent Office

משרד המשפטים
לשכת הפטנטים

This is to certify that annexed hereto is a true copy of the documents as originally deposited with the patent application particulars of which are specified on the first page of the annex.

זאת לתעודה כי רצופים בזה העתקים נכונים של המסמכים שהופקדו לכתחילה עם הבקשה לפטנט לפי הפרטים הרשומים בעמוד הראשון של הנספח.

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

This 14-10-2004 היום

מ. לסרי
ממונה על
רשם הפטנטים
Commissioner of Patents

נתאשר
Certified

0	**For receiving Office use only**	
0-1	International Application No.	**PCT/IL** 2004 / 000806
0-2	International Filing Date	0 7 SEP 2004 (07.09.2004)
0-3	Name of receiving Office and "PCT International Application"	ISRAEL PATENT OFFICE PCT International Application

0-4	**Form PCT/RO/101 PCT Request**	
0-4-1	Prepared Using	PCT-SAFE [EASY mode] Version 3.50 (Build 0002.162)
0-5	**Petition** The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	**Receiving Office (specified by the applicant)**	Israel Patent Office (RO/IL)
0-7	**Applicant's or agent's file reference**	279/04169
I	**Title of Invention**	SECURE MULTICAST TRANSMISSION
II	**Applicant**	
II-1	This person is	applicant only
II-2	Applicant for	all designated States except US
II-4	Name	BAMBOO MEDIACASTING LTD.
II-5	Address	P.O. BOX 5035 44150 KFAR SABA Israel
II-6	State of nationality	IL
II-7	State of residence	IL
II-8	Telephone No.	+972 9 746 4676
II-9	Facsimile No.	+972 9 746 4674
III-1	**Applicant and/or inventor**	
III-1-1	This person is	applicant and inventor
III-1-2	Applicant for	US only
III-1-4	Name (LAST, First)	ENTIN, Leonid
III-1-5	Address	10 ADMONIT STREET 71700 MODIIN Israel
III-1-6	State of nationality	IL
III-1-7	State of residence	IL

III-2	**Applicant and/or inventor**	
III-2-1	This person is	applicant and inventor
III-2-2	Applicant for	US only
III-2-4	Name (LAST, First)	AMRAM, Noam
III-2-5	Address	12 TCHARNIHOVSKI STREET 58382 HOLON Israel
III-2-6	State of nationality	IL
III-2-7	State of residence	IL
III-3	**Applicant and/or inventor**	
III-3-1	This person is	applicant and inventor
III-3-2	Applicant for	US only
III-3-4	Name (LAST, First)	FUCHS, Meir
III-3-5	Address	18/4 NAHAL HAYARKON STREET 71700 MODYIN Israel
III-3-6	State of nationality	IL
III-3-7	State of residence	IL
IV-1	**Agent or common representative; or address for correspondence** The person identified below is hereby/ has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	agent
IV-1-1	Name (LAST, First)	FENSTER, Paul
IV-1-2	Address	FENSTER & COMPANY, INTELLECTUAL PROPERTY 2002 LTD. P. O. BOX 10256 49002 PETACH TIKVA Israel
IV-1-3	Telephone No.	+972 (3) 921-5380
IV-1-4	Facsimile No.	+972 (3) 921-5383
IV-1-5	e-mail	fensterco@fenster.co.il
IV-2	**Additional agent(s)**	additional agent(s) with same address as first named agent
IV-2-1	Name(s)	FENSTER,Maier; ENTIS,Allan; SCHATZ,Yaakov

V	**DESIGNATIONS**		
V-1	**The filing of this request constitutes under Rule 4.9(a), the designation of all Contracting States bound by the PCT on the International filing date, for the grant of every kind of protection available and, where applicable, for the grant of both regional and national patents.**		
VI-1	**Priority claim of earlier national application**		
VI-1-1	Filing date	11 September 2003 (11.09.2003)	
VI-1-2	Number	157886	
VI-1-3	Country	IL	
VI-2	**Priority document request** The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) identified above as ite m(s):	VI-1	
VII-1	**International Searching Authority Chosen**	United States Patent and Trademark Office (USPTO) (ISA/US)	
VIII	**Declarations**	Number of declarations	
VIII-1	Declaration as to the identity of the inventor	-	
VIII-2	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent	-	
VIII-3	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application	-	
VIII-4	Declaration of inventorship (only for the purposes of the designation of the United States of America)	-	
VIII-5	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty	-	
IX	**Check list**	number of sheets	electronic file(s) attached
IX-1	Request (including declaration sheets)	4	✓
IX-2	Description	17	-
IX-3	Claims	7	-
IX-4	Abstract	1	✓
IX-5	Drawings	2	-
IX-7	TOTAL	31	

	Accompanying Items	paper document(s) attached	electronic file(s) attached
IX-8	Fee calculation sheet	✓	-
IX-11	Copy of general power of attorney	✓	-
IX-17	PCT-SAFE physical media	-	✓
IX-19	**Figure of the drawings which should accompany the abstract**	1	
IX-20	**Language of filing of the international application**	English	
X-1	**Signature of applicant, agent or common representative**	Paul Fenster	
X-1-1	Name (LAST, First)	FENSTER, Paul	
X-1-2	Name of signatory		
X-1-3	Capacity		

FOR RECEIVING OFFICE USE ONLY

10-1	**Date of actual receipt of the purported international application**	07 SEP 2004 (07.09.2004)
10-2	**Drawings:**	
10-2-1	Received	✓
10-2-2	Not received	
10-3	**Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application**	
10-4	**Date of timely receipt of the required corrections under PCT Article 11(2)**	
10-5	**International Searching Authority**	ISA/US
10-6	**Transmittal of search copy delayed until search fee is paid**	✓

FOR INTERNATIONAL BUREAU USE ONLY

11-1	**Date of receipt of the record copy by the International Bureau**	

279/04169

PCT REQUEST (ANNEX - FEE CALCULATION SHEET)

Original (for **SUBMISSION**)

(This sheet is not part of and does not count as a sheet of the international application)

0	**For receiving Office use only**	
0-1	International Application No.	PCT/IL2004/000806
0-2	Date stamp of the receiving Office	07 SEP 2004 (07.09.2004)

0-4	**Form PCT/RO/101 (Annex)** **PCT Fee Calculation Sheet**				
0-4-1	Prepared Using		PCT-SAFE [EASY mode] Version 3.50 (Build 0002.162)		
0-9	**Applicant's or agent's file reference**		279/04169		
2	**Applicant**		BAMBOO MEDIACASTING LTD.		
12	**Calculation of prescribed fees**		fee amount/mulipiier	Total amounts (ILS)	Total amounts (USD)
12-1	Transmittal fee	T	⇨	476	
12-2-1	Search fee	S	⇨		1000
12-2-2	International search to be carried out by		US		
12-3	International filing fee (first 30 sheets)	i1	1134 USD		
12-4	Remaining sheets		1		
12-5	Additional amount	(X)	12 USD		
12-6	Total additional amount	i2	12 USD		
12-7	i1 + i2 =	i	1146 USD		
12-12	EASY Filing reduction	R	USD-81		
12-13	Total international filing fee (i-R)	I	⇨		1065
12-14	Fee for priority document Number of priority documents requested		1		
12-15	Fee per document	(X)	0 ILS		
12-16	Total priority document fee:	P	⇨		
12-17	**TOTAL FEES PAYABLE (T+S+I+P)**		⇨	476	2065
12-19	**Mode of payment**		other Please bill us.		

PCT

Original (for SUBMISSION)

13-2-7	Validation messages Contents	Green? Reference number for attached copy of general power of attorney not indicated.

SECURE MULTICAST TRANSMISSION

FIELD OF THE INVENTION

The present invention relates generally to communication networks and particularly to methods of preventing unauthorized dissemination of multicast data.

BACKGROUND OF THE INVENTION

Cellular phones can be used for receiving video clips and other data, in addition to their use for point to point telephone communication. Multicasting the data to the cellular phones or to other mobile stations allows efficient use of the available bandwidth, such that large amounts of data can be provided to the cellular phones without requiring prohibitive amounts of bandwidth. In some cases, users are required to subscribe and pay for the multicast data if they desire to receive the data. In order to prevent other cellular phones that were not subscribed to the data from receiving the data without paying, the data is encrypted and only subscribers are provided with the decryption key. A problem arises, however, if one of the subscribers disseminates the key to other users, allowing the other users to decrypt the data without paying. It is noted that while a subscriber could forward the entire data to other users, this would be very costly in cellular networks, generally more than the cost of subscription.

US patent publication 2003/0046539 to Negawa, the disclosure of which is incorporated herein by reference, suggests periodically changing the key and providing the keys to the subscribers on encrypted private unicast channels. This solution, however, is not suitable for a sophisticated disseminating user who continuously provides the keys to other users immediately when the new keys are received.

US patent publication 2002/0039361, to Hawkes et al., the disclosure of which is incorporated herein by reference, suggests supplying each mobile station with a special processing and storage module which is adapted for storing keys and other secret information, without the information being available to the user for dissemination. Such solution requires that all users buy special hardware in order to receive the multicast data and therefore is unpractical.

US patent publication 2002/0138826 to Peterka, the disclosure of which is incorporated herein by reference, suggests transmitting the multicast data in a few copies with different keys. Each copy of the multicast data is provided with a different rate of changing decryption keys. A subscribing user pays for data for a predetermined amount of time and accordingly is provided with a key for a group having a key replacement timing fitting the time for which the user paid. Thus, change of keys is not required when a user leaves the group. However, no method of discouraging sharing of the keys is described.

US patent publication 2002/0136407, to Denning et al., describes a method of encrypting data such that it can be decrypted only if it passed through a predetermined path, at a predetermined location or during a predetermined time range. The sender encrypts the data directed to each location with an encryption key related to the location of the receiver. This method is not suitable for multicast and is not suggested for multicast.

SUMMARY OF THE INVENTION

An aspect of some embodiments of the invention relates to a method of multicast delivery of a data file to receivers. The method includes encrypting the data file and providing one or more keys required for decrypting the file only after the data is provided to the receiver. Providing the keys only after transmission of the data allows having the receivers request for the keys, so that the requests serve as acknowledgement of receiving the data file.

An aspect of some embodiments of the invention relates to a method of multicasting a data block to a plurality of receivers. The block is represented by a plurality of data segments which include redundancy, such that the block can be determined in its entirety even if fewer than all the segments are received. It is noted that some of the data segments may be identical. The segments are divided into groups which are encrypted using different keys. In order to decrypt the block, the receiver optionally requests, from a control unit, the keys it needs for the segments it received. The segments are transmitted in a manner such that different receivers receive segments requiring different keys and therefore require different sets of keys to decrypt the segments and reconstruct the block. A receiver requesting the keys cannot generally distribute the keys to other receivers on a large scale, as the keys will not be usable, based on statistical analysis, by more than a few other receivers.

In some embodiments of the invention, the keys are transmitted on a high loss channel, such that different receivers receive different segments due to the losses of the channel. Alternatively or additionally, different portions of the segments are transmitted on different channels (e.g., different time slots, frequencies, codes), and different receivers tune on to different channels. Optionally, receivers may tune on to a single channel during the entire transmission or may switch between channels during the transmission. In some embodiments of the invention, each receiver is preconfigured with one or more channels to which it listens.

Further alternatively or additionally, different segments are transmitted in different localities, from different multicasting points, for example from different base stations of a cellular network. A receiver may optionally regenerate the block using a valid set of segments collected from a plurality of different multicasting points, and is not limited to segments from a single multicasting point. Thus, a receiver moving during the transmission between different multicasting points can use the data received from different multicast points.

The data segments are optionally generated and encrypted at a single source point, and are transmitted from the source point to the multicasting points on respective unicast channels, optionally passing on cables connecting the source point to the multicast points. As the cost of wireless bandwidth is much higher than the cost of terrestrial bandwidth, the additional cost of distributing different segments or different keys to the multicast points by land lines is relatively small.

Alternatively, the segments are not encrypted (or are encrypted using a different method) on their way to the multicasting points, and the encryption is performed by the multicasting points. In this alternative, the segments may be multicast to the multicasting points, over a cabled network or wirelessly using encryption or frequencies not available to the end user, thus reducing the amount of bandwidth used for distributing the data to the multicasting points. Further alternatively, the data is broken up into segments or is generated at the multicasting points or on the way to the multicasting points.

In some embodiments of the invention, the segments representing the block include FEC encrypted segments, such that a receiver collecting a predetermined number (m) of segments out of the (n) transmitted segments can reconstruct the block. Optionally, sub-groups of the FEC segments, including one or more segments, are encrypted with different keys. If many of the receivers receive the block on a high loss rate channel, such that they receive only m or a few more than m segments, the receivers will generally require different sets of keys for decryption.

Optionally, the keys are changed with time, for example after transmission of every few segments. Alternatively, the segments encrypted with same keys are interleaved between segments encrypted with other keys.

In some embodiments of the invention, the encryption segments are smaller than or equal the size of the FEC segments, such that they do not extend beyond the border between two FEC segments. Thus, an error in a transmitted encryption segment affects only a single FEC segment.

The methods for discouraging key sharing of the present invention may optionally be used with substantially any coding method, from very simple methods to very complex methods. It is noted, however, that using the methods of the present invention serves in itself as a relatively high barrier to illegitimate decryption on a large scale and therefore, relatively simple coding methods, such as symmetric encryption may be used.

The methods of the present invention are generally applied to the data itself and not to keys which are used to encrypt the data. Therefore, a user who rightfully receives the keys to the data cannot easily transfer the decrypted data to a different user, as this would require transferring very large amounts of data.

An aspect of some embodiments of the present invention relates to transmitting same multicast data through a plurality of base stations with different encryption for each of the base stations. In some embodiments of the invention, a mobile station receiving a first portion of the data from a first base station and a second portion of the data from a second base station can reconstruct the data, although the first and second portions were encrypted with different encryption. The different encryption optionally includes use of a different key and/or a different encryption method. Using different encryption schemes for data transmitted by different base stations, limits the possibility of illegal disseminating decryption keys, as keys suitable for data of one base station are not suitable for other base stations.

There is therefore provided, in accordance with an embodiment of the invention, a method of multicasting data, comprising providing a data block for multicasting, generating a plurality of segments that represent the data block, such that a receiver needs to receive fewer than all the generated segments in order to reconstruct the data block, encrypting at least a portion of the generated segments, so as to generate encrypted data units encrypted with a plurality of different keys or encryption methods and transmitting the encrypted data units over one or more multicast channels.

Optionally, generating the plurality of segments comprises generating forward error correction (FEC) segments, such that any group of a predetermined number of non-identical segments can be used to reconstruct the data block. Optionally, generating the plurality of segments comprises generating segments that include a portion of the data block.

Optionally, the plurality of segments include at least one set of duplicate segments.

Optionally, encrypting at least a portion of the segments comprises encrypting such that each data unit represents data from a single segment. Optionally, encrypting at least a portion of the segments comprises encrypting each segment into a single encrypted data unit. Alternatively or additionally, encrypting at least a portion of the segments comprises encrypting data of each segment into a plurality of encrypted data units. Optionally, encrypting data of each segment into a plurality of encrypted data units comprises leaving a portion of each segment not encrypted. Optionally, the non-encrypted portions of the segments are used for transferring preview information. Optionally, the non-encrypted portions are located in different positions in different segments. Alternatively, the non-encrypted portions are located in same positions of substantially all the segments.

Optionally, encrypting at least a portion of at least some of the segments comprises encrypting using a symmetric coding scheme. Optionally, encrypting using a plurality of different keys or methods comprises encrypting using different keys and substantially same methods. Alternatively or additionally, encrypting using a plurality of different keys or methods comprises encrypting using different methods. Optionally, transmitting the encrypted data units comprises transmitting through a plurality of transmission points each of which transmits to different areas. Optionally, transmitting the encrypted data units comprises transmitting through a plurality of base stations. Optionally, each transmission point transmits sufficient data required for reconstruction of the data block.

Optionally, at least some of the transmission points transmit data units representing identical segments encrypted using different keys or methods. Optionally, the transmission points of at least one group of two or more transmission points transmit data units representing identical segments encrypted using same keys and methods. In some embodiments of the invention, the transmission points included in a group that transmit data units representing identical segments encrypted using same keys and methods vary dynamically over time.

Optionally, at least one of the transmission points transmits data units encrypted using a plurality of different keys or methods. Optionally, the encrypted data units are transmitted along with an identification of the respective key required to decrypt the data unit. Optionally, the identification of the key includes a portion which depends on the transmission point through which the data unit is transmitted. Optionally, the encrypted data units are transmitted along with an identification of the respective key required to decrypt the data unit. Optionally, the identification of the key is included in a field including redundancy, such that only some of the possible values of the field are valid identifications of keys. Optionally, encrypting at least a portion of the generated segments comprises encrypting with a sufficient number of keys, so that given a loss rate of the multicast channels, less than a predetermined percentage of receivers of the data block will require, on the average, the same set of keys for decryption.

Optionally, encrypting at least a portion of the generated segments comprises encrypting with a sufficient number of keys, so that given a loss rate of the multicast channels, less than ten percent of the receivers of the data block will require on the average the same set of keys for decryption. Optionally, encrypting at least a portion of the generated segments comprises encrypting with a sufficient number of keys, so that given a loss rate of the multicast channels, less than one percent of the receivers of the data block will require on the average the same set of keys for decryption. Optionally, the method includes receiving requests for keys required for decryption and keeping track of receivers that request a suspiciously large number of keys and/or request keys corresponding to non-existent identifications. Optionally, substantially all the encryption is performed at the same unit. Alternatively, the encryption of different segments is performed by different units.

There is further provided in accordance with an embodiment of the invention, a method of receiving multicast data over a transmission network, by a mobile station, comprising receiving one or more data units of a data block, from each of a plurality of multicast transmission points, the data units of each transmission point being encrypted using different respective one or more keys, decrypting the data units and reconstructing the data block from the decrypted data units, which were received from the plurality of multicast transmission points.

Optionally, the method includes determining from the received data units identification of the keys required in order to decrypt the data units and requesting the required keys from a key server. Optionally, the identifications of the keys depend, at least partially, on the multicast transmission point through which the data units are received, such that data units transmitted through different transmission points include different key identifications. Optionally, the multicast transmission points include base stations and/or wireless LAN access points.

There is further provided in accordance with an embodiment of the invention, a method of multicasting data, comprising providing a data block for multicasting, generating a plurality of different sets of encrypted segments requiring different sets of decryption keys, to represent the data block, and transmitting each of the different sets of encrypted segments from a different multicast transmission point.

Optionally, generating the plurality of different sets of encrypted segments comprises generating a single set of non-encrypted segments and generating the plurality of different sets of encrypted segments by encrypting the non-encrypted segments using a plurality of different encryption keys. Optionally, generating the plurality of different sets of encrypted segments comprises encrypting each of the plurality of different sets using groups of different keys. Optionally, the groups of different keys do not include any common keys. Optionally, the transmission points comprise base stations of a cellular network. Optionally, generating the plurality of different sets of encrypted segments is performed in a single encryption unit. Optionally, at least part of the generating of the sets of encrypted segments is performed separately for each set in respective processors associated with the transmission points. Optionally, each of the encrypted segments includes a key identification field which identifies the key required to decrypt the segment.

Optionally, the method includes providing keys required for decrypting a plurality of sets of segments to a single receiver. Optionally, the method includes providing no more than 50% of the keys used for segments related to the data block to any single receiver.

There is further provided in accordance with an embodiment of the invention, a method of multicasting data, comprising providing a data block, generating a plurality of segments that represent the data block, such that a receiver needs to receive fewer than all the generated segments in order to reconstruct the data block, encrypting a portion of each of the generated segments, so as to generate respective transmission segments including both encrypted and non-encrypted data and transmitting the transmission data units over a multicast channel.

There is further provided in accordance with an embodiment of the invention, a method of multicast transmission comprising providing a data block, encrypting the data block utilizing at least one given key, multicast transmitting the encrypted data block, requesting the at least one key by a receiver that receives the encrypted data block and unicast transmitting the at least one key to the receiver.

Optionally, encrypting the data block comprises generating a plurality of segments that represent the data block, such that a receiver needs to receive fewer than all the generated segments in order to reconstruct the data block and encrypting at least some of the segments.

Optionally, encrypting at least some of the segments comprises encrypting one or more of the segments utilizing a first key and using at least one other key for at least one other segment. Optionally, requesting the at least one key comprises requesting based on an identification of the key included in the transmission. Optionally, the identification of the key is included in a field that can receive more values than valid identification values. Optionally, the method includes identifying receivers that request a suspiciously large number of keys or request non-existent keys. Optionally, requesting the at least one key is performed only after the receiver determined that a sufficient amount of data was received to allow reconstruction of the data block.

BRIEF DESCRIPTION OF FIGURES

Particular non-limiting embodiments of the invention will be described with reference to the following description of embodiments in conjunction with the figures. Identical structures, elements or parts which appear in more than one figure are preferably labeled with a same or similar number in all the figures in which they appear, in which:

Fig. 1 is a schematic illustration of a cellular network, useful in explaining an exemplary embodiment of the present invention; and

Fig. 2 is a flowchart of acts performed by a mobile station in receiving a file, in accordance with an exemplary embodiment of the invention.

DETAILED DESCRIPTION OF EMBODIMENTS

Fig. 1 is a schematic illustration of a cellular network 100, in accordance with an exemplary embodiment of the present invention. Network 100 includes a plurality of base stations 50, which transmit signals to mobile stations 20 in their vicinity. In transmission of multicast data to mobile stations 20, a data source 30 generates files which are to be multicast to subscribing mobile units 20. Optionally, the generated files are broken into blocks of predetermined size, suitable for processing. The blocks are optionally passed to a forward error correction (FEC) unit 32, where a plurality of segments are prepared to represent the block. Optionally, N segments are prepared, such that any M (M<N) of the N segments can be used to reconstruct the block. The FEC segments may be generated using substantially any FEC method known in the art, including one-dimensional, two-dimensional, systematic and non-systematic methods. In an exemplary embodiment of the invention, a FEC method such as described in PCT patent application PCT/IL2004/000204, filed March 3, 2004 and/or in Israel patent application 157,885, titled "Iterative Forward Error Correction", filed September 11, 2003, the disclosures of which are incorporated herein by reference, is used. The FEC segments are optionally transferred to an encryption unit 34, which encrypts the FEC segments, forming respective encrypted segments.

The encrypted segments of each base station 50 are optionally transferred through a terrestrial network 40 of cellular network 100 to their intended base station, from which they are transmitted to mobile stations 20. Base stations 50 operate as multicast transmission points from which transmitted segments of the same data are all identical. The segments from data source 30 to base stations 50 may be different for different segments although they carry the same data. The segments are transmitted to mobile stations 20 using any multicast method known in the art, such as the method described in PCT publication WO03/019840 published

March 6, 2003, the disclosure of which is incorporated herein by reference. Optionally, each encrypted segment is transmitted as a respective RLC segment using methods known in the art.

Network 100 optionally includes a key server 36 which provides decryption keys to mobile stations 50. In some embodiments of the invention, users receiving the block (or the entire file), desiring to read the block, contact key server 36 and request the keys they need for the decryption. Alternatively or additionally, some of the keys are provided in multicast, and the users request only the keys that they need which were not multicast to them.

In some embodiments of the invention, for each base station 50, encryption unit 34 prepares differently encrypted segments, using keys which are different from those for the other base stations. Alternatively or additionally, some base stations use the same keys or use partially overlapping groups of keys, in order to limit the number of keys managed by encryption unit 34. Optionally, base stations separated by large distances use the same keys or a partial group of overlapping keys. Alternatively or additionally, base stations generally having small numbers of users use keys which are also used by other base stations. Further alternatively or additionally, all base stations 50 in a same region and/or controlled by a same controller, e.g., a same point-to-multipoint unit PTMU (introduced below) and/or base station controller (BSC), use the same keys.

Optionally, the size of a region of base stations that use the same keys is selected such that a moving mobile will not pass through more than a predetermined number (e.g., 10-20) regions having different keys, so as to limit the number of keys that moving receivers need to request. In some embodiments of the invention, when a region uses more than one key for a single file, the total number of keys that a moving receiver will need to request is limited to less than a predetermined number of keys (e.g., less than 20, 30 or 50). Optionally, the sizes of the regions that have the same keys depend on the expected movement speed of the receiver. For regions in which fast movement is allowed through a large number of cells (i.e., areas governed by respective base stations), the number of neighboring base stations sharing common keys is relatively large (e.g., greater than 10-20). Conversely, in regions in which movement is relatively slow and/or cells are relatively large, the number of cells sharing keys is relatively small (e.g., smaller than 10 or even 6).

Alternatively to sharing keys by neighboring cells, the cells that share keys are close cells that are separated by one or more intervening cells. Thus, a moving receiver does not need many keys, but neighboring receivers cannot necessarily use the same keys.

In some embodiments of the invention, base stations sharing keys share all their keys. Alternatively or additionally, some or all base stations that share keys share only some of their keys.

The base stations that share keys may be predetermined groups of base stations. Alternatively, in order to make unauthorized dissemination of keys more difficult, the grouping of the base station using same keys varies in real time. In some embodiments of the invention, the base station grouping varies every few hours or days. Alternatively, the base station groupings change every few moments and/or for every transmitted message or for every small number (e.g., up to 5-10) of messages. Further alternatively or additionally, the base station groupings may be changed within the transmission of a single message.

In some embodiments of the invention, the grouping of the base stations is changed randomly or in a pseudo random manner in order to prevent hackers from determining the grouping patterns. Alternatively or additionally, the grouping is adjusted according to the load on the network. Optionally, when the network is relatively loaded, fewer keys are used, for example having adjacent base stations use the same keys. This reduces the amount of bandwidth required for disseminating the keys and for providing the data to the base stations. When the network is relatively not loaded, more keys are used, to allow for better protection of the data. Alternatively or additionally, the local diversity of encryption keys is configurable by a network operator.

Each base station 50 optionally uses a plurality of different keys for the segments of a single block. The number of keys used in encrypting the data of a single block for a single base station 50 is optionally determined as a compromise between using a large number of keys required for key diversity which prevents illegitimate dissemination of keys and a small number of keys, which reduces the amount of bandwidth spent on dissemination of keys to users. In an exemplary embodiment of the invention, a different key is used for about every 10-20 segments. Optionally, segments that are encrypted with the same key include sequential portions of data from the block. This option reduces the number of keys a user requires on the average. Therefore, users requiring a large number of keys raise more suspicion that they disseminate keys to others. Alternatively, segments encrypted with the same key are taken from separated portions of the block such that the segments encrypted with a single key are interleaved between segments encrypted with other keys.

In some cases, some or all of the data segments of the block are transmitted a plurality of times in order to ensure proper reception, for example when mobile stations 20 may tune onto the channel at different times. Optionally, each time the segments are transmitted they are encrypted with different keys.

In some embodiments of the invention, each transmitted segment includes a header which states the block and/or file to which it belongs, the position of the segment in an FEC array representing the block and an ID of the key required for decryption. The header is optionally not encrypted, so that the receiver can determine which segments are duplicates and can be discarded, whether a sufficient number of segments were received for reconstruction of the block and which keys are required for decrypting the segments. Alternatively or additionally, the segments are included in larger packets, for example IP packets, and the control information of the segment is included in a control section of the IP packet including the segment.

Optionally, the segment headers also include general information on the FEC method and/or encryption method. Alternatively or additionally, the general information is provided in the IP packets and/or at the beginning of the multicast. Further alternatively or additionally, the general information is provided on a separate channel, such as a broadcast channel describing the available multicast data and/or on a separate unicast channel used to provide the keys or for providing data at the beginning of the transmission.

Although data source 30, FEC unit 32, encryption unit 34 and key server 36 are shown as separate units, in some embodiments of the invention, one or more of these units are implemented by a single entity. For example, encryption unit 34 and key server 36 may be implemented on a single processor and/or may use a common key database. In some embodiments of the invention, data source 30 performs the task of FEC unit 32 and/or encryption unit 34 before forwarding the packets. In other embodiments of the invention, the encryption is performed at base stations 50 or at processors associated with each of the base stations. For example, the encryption may be performed at point to multi-point units (PTMUs) of the base stations, which PTMUs are described in the above mentioned PCT patent application PCT/IL2004/000204. Optionally, in these embodiments, the encryption ID is generated by each base station and/or PTMU from a static (i.e., changes infrequently if at all) code of the base station and a time dependent code which may be common to all base stations or is generated separately for each base station. Optionally, the static code is kept secret from the users, to make it harder on users to guess the encryption keys.

In some embodiments of the invention, two or more of the entities of network 100, for example encryption unit 34 and base stations 50, have the ability to encrypt the segments. The unit that actually performs the encryption at any specific time optionally depends on the available processing resources on the units. For example, when the base stations are very loaded, the encryption is optionally performed by encryption unit 34.

Fig. 2 is a flowchart of acts performed by a mobile station in receiving a file, in accordance with an exemplary embodiment of the invention. The mobile station optionally tunes onto a multicast channel and receives (204) encrypted segments. The mobile station optionally verifies (206) that the packets were received without error. For example, the segments may include a CRC field, the value of which is used to check that the segment was received intact. The CRC check may be performed by an application layer performing the decryption and reconstruction or by a lower protocol layer. Segments that were received without error are optionally stored (208) in a memory of the mobile station. When a group of segments sufficient to allow reconstruction of a block is accumulated, the mobile station transmits (210) a message to key server 36, with IDs of the keys it requires in order to decrypt the segments it received. Optionally, the receiver knows that a sufficient number of packets were received when a predetermined number of packets sufficient for reconstruction were received. Alternatively, the receiver simulates the reconstruction, without actually performing the reconstruction which cannot be performed without the keys, in order to determine whether a sufficient number of packets were received. The simulations are optionally performed as described in the above mentioned Israel patent application 157,885.

Key server 36 transmits the keys generally on a unicast transmission, to the mobile station (211), which uses the keys to decrypt (212) the segments. Optionally, the keys are transmitted in a compressed format. The block is then reconstructed (214) from the decrypted segments according to the FEC method used.

In some embodiments of the invention, in storing (208) the received segments, the mobile unit discards segments carrying the same data (even if the segments were encrypted with a different encryption). Optionally, in any case a duplicate segment is received, the later received segment is discarded. Alternatively, if one of the duplicate segments can be opened with the same key as a different segment already received, the other copy of the duplicate segment is discarded. In some embodiments of the invention, a user not receiving a sufficient number of multicast segments required for reconstruction during the multicast transmission may request supplement of data on a unicast link, for example along with requesting the keys.

Key server 36 optionally keeps track of the mobile stations requesting keys, for billing purposes. In some embodiments of the invention, key server 36 keeps special track of mobile stations that request particularly large sets of keys. Optionally, the content provider checks users that persistently, for many files, request large numbers of keys, to determine if they disseminate the keys to other users who are not being billed. In an exemplary embodiment of the invention, each file is transmitted 3-5 times with a 40-100% redundancy. In accordance with this exemplary embodiment, a request for about 25-30% of the keys is considered reasonable.

Alternatively or additionally to checking the number of keys requested, key server 36 checks whether there is a possibility that the requesting mobile station actually needs all the keys requested by the mobile station. For example, a mobile station requesting keys belonging to packets transmitted in locations separated by a distance which cannot be traveled during the entire transmission time of the file would be considered suspicious. In some embodiments of the invention, when a mobile station requests two keys which can only be used for the same segment (with different encryption) the reason is enquired.

Optionally, when a suspicious request for keys is received, an alarm message is sent to a controller of network 100. Alternatively or additionally, a periodic report on suspicious key requests is initiated. In some embodiments of the invention, location data on the mobile station initiating the suspicious request for keys is determined.

In some embodiments of the invention, the key IDs associated with the segments that are transmitted to key server 36 in requesting the keys, are not allocated in any consecutive order, but rather are selected randomly. This makes requesting keys for segments that the user did not receive, in order to disseminate the keys to other users who do not pay for the keys, harder. Optionally, the key IDs have a length which is sufficient to allow use of only some of the possible values in the keys, so as to make it more difficult for users to guess key IDs. Optionally, a manager of the network follows up on users that request non-existing keys. The length of the key ID field is optionally selected as a compromise between a long length which reduces the chances of illegal key dissemination and a short length which reduces the bandwidth required for key IDs. In an exemplary embodiment of the invention, the segment headers add an overhead of about 1-2%.

Alternatively to a single number serving as the key ID, the key ID may be formed of a plurality of fields, such as a first field identifying the base station 50 and a second field identifying the specific key used for the specific segment.

In some embodiments of the invention, different key IDs are used to represent the same key. This gives the advantage of using less bandwidth for providing the keys, while not allowing the subscribers to know before asking for the keys that the keys are the same. For example, different cells may use different key IDs for same keys used in common by the cells.

Optionally, mobile stations do not request (210) any keys unless they received sufficient data to allow reconstruction of the block. Thus, the mobile station is not billed for the block or for a file unless the block was received in a manner which allows reconstruction. This prevents billing mobile stations for data they could not reconstruct, for example due to an interference in communications between the base station and the mobile station in the middle of multicast data reception.

Alternatively to transmitting (211) all the required keys to the mobile station after all the data was received by the mobile stations, some or all of the keys are provided before the multicast transmission and/or along with the multicast transmission. In some embodiments of the invention, some of the keys are provided in a multicast transmission.

The implementation of the present invention allows using relatively simple encryption methods, since in order to reconstruct a file the receiver needs to break the code for a plurality of different keys. In addition, even if a subscriber succeeds in breaking the code and determining the keys for the data it received, most other users cannot reconstruct the file using these keys as they need other keys. In some embodiments of the invention, the encryption method used is sufficiently complex to prevent breaking of the code by small processors, such as hosted by mobile stations 20, but which may be breakable by stronger processors not usually hosted by mobile units. In some embodiments of the invention, the encryption is performed using a single key for both encryption and decryption. Encryption schemes using a single key for encryption and decryption require less processing resources for decryption, than public-private schemes, so that the battery of the mobile units is not drained out too fast.

Optionally, the encryption is performed in accordance with a polynomial encryption method. Alternatively or additionally, the encryption is performed using a low density parity code (LDPC) such as the Tornado code. Alternatively, the encryption is performed using a public/private key scheme. In some embodiments of the invention, when it is desired to minimize the processing power spent on decryption, a low-complexity encryption scheme is used. For example, a streaming encryption scheme based on generator polynomials may be used.

It is noted that when the channel between base stations 50 and mobile stations 20 has a high loss rate, for example, due to high noise levels and/or late tuning of mobile stations 20 onto the channel, the chances of several mobile stations 20 requiring exactly the same keys is very small. Optionally, the number of keys used is set such that on the average no more than 5-10 users require the same keys. Alternatively or additionally, the number of keys used is selected such that, on the average, in each cell no more than 5-10% of the receivers require the same keys. Further alternatively or additionally, the number of keys used is selected, such that no more than 0.1-1% of the receivers in the network, on the average, require the same set of keys. Further alternatively or additionally, the number of keys used is adjusted according to the importance of the encrypted data.

In the above description, the same encryption methods are used for all the base stations at all times, but with different keys. Alternatively, the encryption methods are varied from time to time in order to make the breaking of the code more difficult. In some embodiments of the invention, each mobile station 20 optionally has software that can decrypt a plurality of different codes. Along with each key received from key server 36, the receiver is optionally provided with identification of a decryption method to be used with the key.

Alternatively to encrypting segments of the same size as the FEC segments, the encryption may be performed on smaller segments. In some embodiments of the invention, the encryption segments do not range over the border between two FEC segments, so that an error in a transmitted encryption segment affects only a single FEC segment.

In an exemplary embodiment of the invention, the DES encryption algorithm is used. The DES encryption algorithm operates on encryption segments of 8 bytes. Optionally, the FEC segments are larger than the encryption segments, for example including 30 bytes in each segment. In some embodiments of the invention, each FEC segment is broken into four portions: three encrypted segments of 8 bytes each, and a non-encrypted segment of 6 bytes.

In some embodiments of the invention, the non-encrypted bytes are located in the same positions of the FEC segments, such that the receivers can determine 20% of the data without decryption. Optionally, these embodiments are used when 20% of the data file cannot be used without the rest of the data. Alternatively or additionally, at least some of the 20% of the data is used to transfer previews, ads and/or other data which is to be supplied to the users for free. Alternatively, the non-encrypted bytes are positioned at different positions in the FEC segments for different FEC segments. Using a substantially even distribution, each position carries 80% encrypted data and 20% unencrypted data. Thus, for each position, a receiver without encryption keys has at most 20% of the data, if no data is lost. This alternative is optionally used when it is not possible to reconstruct the file only with the unencrypted data. It is noted that although the above discussion uses specific numbers for the unencrypted portion, the principals of the invention may be used also for other ratios between encrypted and non-encrypted data in the FEC segments.

Although the above description relates to using FEC segments, the present invention may be used with other redundancy methods, such as duplication and/or repeated transmission on different channels and/or in different locations.

The above description relates to base stations that serve as multicast transmission points. It is noted that the present invention may be used for other types of multicast transmission points, such as wireless local area network (WLAN) access points. It is noted that the present invention may be used also in networks that have a plurality of different types of multicast transmission points. Furthermore, the present invention may be used with one or more transmission points that transmit signals on a plurality of different channels (e.g., frequency or code channels), each of the channels defining a separate respective cell.

It will be appreciated that the above described methods may be varied in many ways, including, changing the order of steps, and the exact implementation used. The methods of the present invention may be performed in various protocol layers and may be performed for a single transmission system in a plurality of communication protocol layers. It should also be appreciated that the above described methods and apparatus are to be interpreted as including apparatus for carrying out the methods and methods of using the apparatus.

The present invention has been described using non-limiting detailed descriptions of embodiments thereof that are provided by way of example and are not intended to limit the scope of the invention. For example, different keys may be used only for different base stations without changing the keys for different segments of the same block from a same base station. Thus, the bandwidth required for key dissemination is small while risking a local illegal dissemination of keys. It should be understood that features and/or steps described with respect to one embodiment may be used with other embodiments and that not all embodiments of the invention have all of the features and/or steps shown in a particular figure or described with respect to one of the embodiments. Variations of embodiments described will occur to persons of the art.

It is noted that some of the above described embodiments may describe the best mode contemplated by the inventors and therefore may include structure, acts or details of structures and acts that may not be essential to the invention and which are described as examples. Structure and acts described herein are replaceable by equivalents which perform the same function, even if the structure or acts are different, as known in the art. Therefore, the scope of the invention is limited only by the elements and limitations as used in the claims. When used in the following claims, the terms "comprise", "include", "have" and their conjugates mean "including but not limited to".

CLAIMS

1. A method of multicasting data, comprising:

providing a data block for multicasting;

generating a plurality of segments that represent the data block, such that a receiver needs to receive fewer than all the generated segments in order to reconstruct the data block;

encrypting at least a portion of the generated segments, so as to generate encrypted data units encrypted with a plurality of different keys or encryption methods; and

transmitting the encrypted data units over one or more multicast channels.

2. A method according to claim 1, wherein generating the plurality of segments comprises generating forward error correction (FEC) segments, such that any group of a predetermined number of non-identical segments can be used to reconstruct the data block.

3. A method according to claim 1, wherein generating the plurality of segments comprises generating segments that include a portion of the data block.

4. A method according to claim 1, wherein the plurality of segments include at least one set of duplicate segments.

5. A method according to claim 1, wherein encrypting at least a portion of the segments comprises encrypting such that each data unit represents data from a single segment.

6. A method according to claim 1, wherein encrypting at least a portion of the segments comprises encrypting each segment into a single encrypted data unit.

7. A method according to claim 1, wherein encrypting at least a portion of the segments comprises encrypting data of each segment into a plurality of encrypted data units.

8. A method according to claim 7, wherein encrypting data of each segment into a plurality of encrypted data units comprises leaving a portion of each segment not encrypted.

9. A method according to claim 8, wherein the non-encrypted portions of the segments are used for transferring preview information.

10. A method according to claim 8, wherein the non-encrypted portions are located in different positions in different segments.

11. A method according to claim 8, wherein the non-encrypted portions are located in same positions of substantially all the segments.

12. A method according to claim 1, wherein encrypting at least a portion of at least some of the segments comprises encrypting using a symmetric coding scheme.

13. A method according to claim 1, wherein encrypting using a plurality of different keys or methods comprises encrypting using different keys and substantially same methods.

14. A method according to any of claims 1-12, wherein encrypting using a plurality of different keys or methods comprises encrypting using different methods.

15. A method according to any of claims 1-12, wherein transmitting the encrypted data units comprises transmitting through a plurality of transmission points each of which transmits to different areas.

16. A method according to claim 15, wherein transmitting the encrypted data units comprises transmitting through a plurality of base stations.

17. A method according to claim 15, wherein each transmission point transmits sufficient data required for reconstruction of the data block.

18. A method according to claim 15, wherein at least some of the transmission points transmit data units representing identical segments encrypted using different keys or methods.

19. A method according to claim 18, wherein the transmission points of at least one group of two or more transmission points transmit data units representing identical segments encrypted using same keys and methods.

20. A method according to claim 19, wherein the transmission points included in a group that transmit data units representing identical segments encrypted using same keys and methods vary dynamically over time.

21. A method according to claim 20, wherein the transmission points included in a group that transmit data units representing identical segments encrypted using same keys or methods vary during transmission of data units representing a single data block.

22. A method according to claim 15, wherein at least one of the transmission points transmits data units encrypted using a plurality of different keys or methods.

23. A method according to claims 15, wherein the encrypted data units are transmitted along with an identification of the respective key required to decrypt the data unit.

24. A method according to claim 23, wherein the identification of the key includes a portion which depends on the transmission point through which the data unit is transmitted.

25. A method according to claim 1, wherein the encrypted data units are transmitted along with an identification of the respective key required to decrypt the data unit.

26. A method according to claim 25, wherein the identification of the key is included in a field including redundancy, such that only some of the possible values of the field are valid identifications of keys.

27. A method according to claim 1, wherein encrypting at least a portion of the generated segments comprises encrypting with a sufficient number of keys, so that given a loss rate of the multicast channels, less than a predetermined percentage of receivers of the data block will require, on the average, the same set of keys for decryption.

28. A method according to claim 27, wherein encrypting at least a portion of the generated segments comprises encrypting with a sufficient number of keys, so that given a loss rate of the multicast channels, less than ten percent of the receivers of the data block will require on the average the same set of keys for decryption.

29. A method according to claim 28, wherein encrypting at least a portion of the generated segments comprises encrypting with a sufficient number of keys, so that given a loss rate of the multicast channels, less than one percent of the receivers of the data block will require on the average the same set of keys for decryption.

30. A method according to claim 1, comprising receiving requests for keys required for decryption and keeping track of receivers that request a suspiciously large number of keys and/or request keys corresponding to non-existent identifications.

31. A method according to claim 1, wherein substantially all the encryption is performed at the same unit.

32. A method according to any of claims 1-12, wherein the encryption of different segments is performed by different units.

33. A method of receiving multicast data over a transmission network, by a mobile station, comprising:

receiving one or more data units of a data block, from each of a plurality of multicast transmission points, the data units of each transmission point being encrypted using different respective one or more keys;

decrypting the data units; and

reconstructing the data block from the decrypted data units, which were received from the plurality of multicast transmission points.

34. A method according to claim 33, comprising determining from the received data units identification of the keys required in order to decrypt the data units and requesting the required keys from a key server.

35. A method according to claim 34, wherein the identifications of the keys depend, at least partially, on the multicast transmission point through which the data units are received, such that data units transmitted through different transmission points include different key identifications.

36. A method according to claim 33, wherein the multicast transmission points comprise base stations.

37. A method according to claim 33, wherein the multicast transmission points comprise one or more wireless LAN access points.

38. A method of multicasting data, comprising:

providing a data block for multicasting;

generating a plurality of different sets of encrypted segments requiring different sets of decryption keys, to represent the data block; and

transmitting each of the different sets of encrypted segments from a different multicast transmission point.

39. A method according to claim 38, wherein generating the plurality of different sets of encrypted segments comprises generating a single set of non-encrypted segments and generating the plurality of different sets of encrypted segments by encrypting the non-encrypted segments using a plurality of different encryption keys.

40. A method according to claim 38, wherein generating the plurality of different sets of encrypted segments comprises encrypting each of the plurality of different sets using groups of different keys.

41. A method according to claim 40, wherein the groups of different keys do not include any common keys.

42. A method according to claim 40, wherein the transmission points comprise base stations of a cellular network.

43. A method according to claim 40, wherein generating the plurality of different sets of encrypted segments is performed in a single encryption unit.

44. A method according to claim 40, wherein at least part of the generating of the sets of encrypted segments is performed separately for each set in respective processors associated with the transmission points.

45. A method according to claim 38, wherein each of the encrypted segments includes a key identification field which identifies the key required to decrypt the segment.

46. A method according to claim 38, comprising providing keys required for decrypting a plurality of sets of segments to a single receiver.

47. A method according to claim 38, comprising providing no more than 50% of the keys used for segments related to the data block to any single receiver.

48. A method of multicasting data, comprising:

providing a data block;

generating a plurality of segments that represent the data block, such that a receiver needs to receive fewer than all the generated segments in order to reconstruct the data block;

encrypting a portion of each of the generated segments, so as to generate respective transmission segments including both encrypted and non-encrypted data; and

transmitting the transmission data units over a multicast channel.

49. A method of multicast transmission comprising:

providing a data block;

encrypting the data block utilizing at least one given key;

multicast transmitting the encrypted data block;

requesting the at least one key by a receiver that receives the encrypted data block; and

unicast transmitting the at least one key to the receiver.

50. A method according to claim 49, wherein encrypting the data block comprises generating a plurality of segments that represent the data block, such that a receiver needs to

receive fewer than all the generated segments in order to reconstruct the data block and encrypting at least some of the segments.

51. A method according to claim 50, wherein encrypting at least some of the segments comprises encrypting one or more of the segments utilizing a first key and using at least one other key for at least one other segment.

52. A method according to claim 49, wherein requesting the at least one key comprises requesting based on an identification of the key included in the transmission.

53. A method according to claim 52, wherein the identification of the key is included in a field that can receive more values than valid identification values.

54. A method according to claim 49, comprising identifying receivers that request a suspiciously large number of keys or request non-existent keys.

55. A method according to claim 49, wherein requesting the at least one key is performed only after the receiver determined that a sufficient amount of data was received to allow reconstruction of the data block.

ABSTRACT

A method of multicasting data. The method includes providing a data block for multicasting, generating a plurality of segments that represent the data block, such that a receiver needs to receive fewer than all the generated segments in order to reconstruct the data block, encrypting at least a portion of the generated segments, so as to generate encrypted data units encrypted with a plurality of different keys or encryption methods and transmitting the encrypted data units over one or more multicast channels.

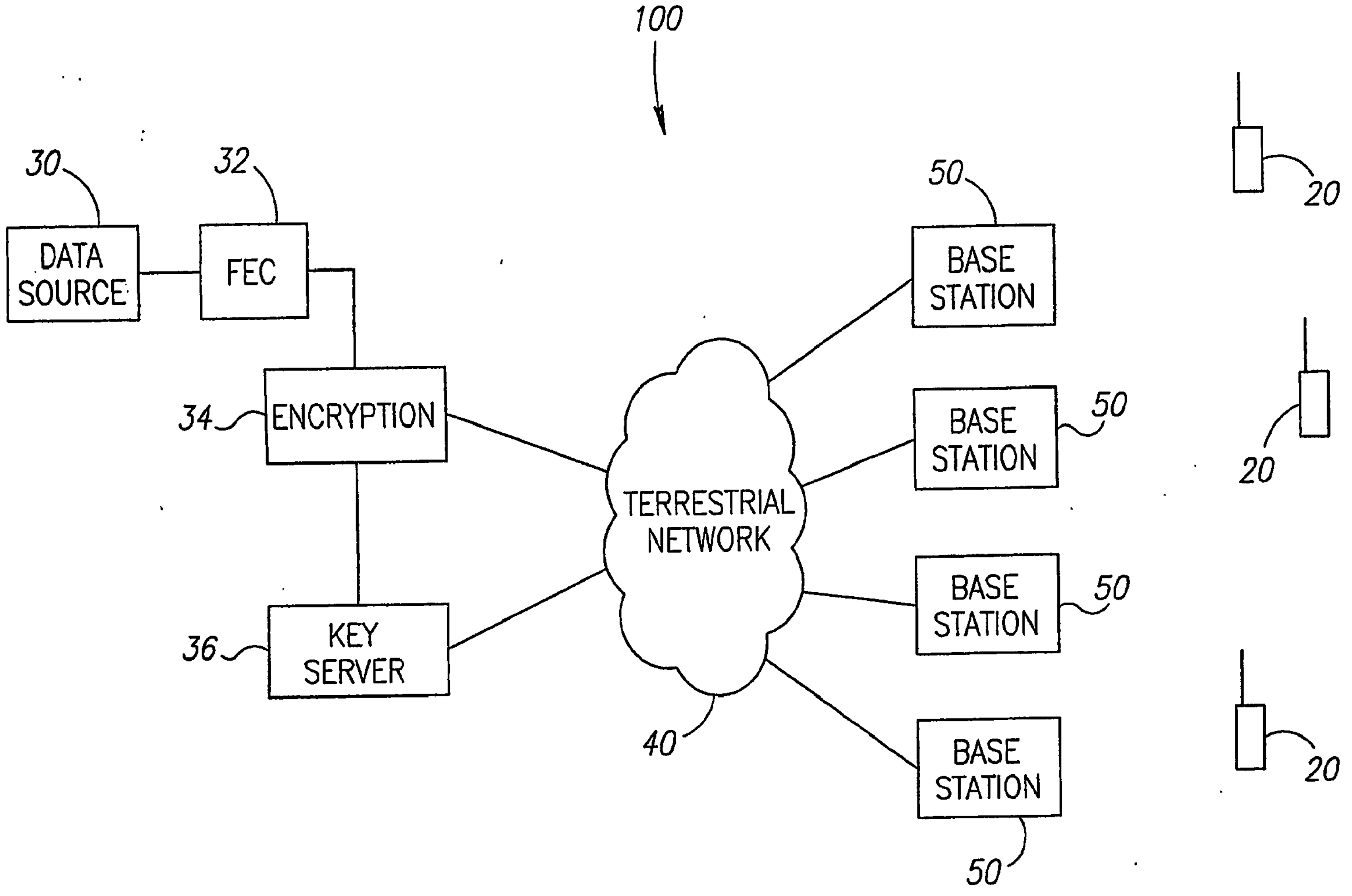
100
30
DATA SOURCE
32
FEC
34
ENCRYPTION
36
KEY SERVER
TERRESTRIAL NETWORK
40
50
BASE STATION
50
BASE STATION
50
BASE STATION
50
BASE STATION
50
20
20
20

FIG.1

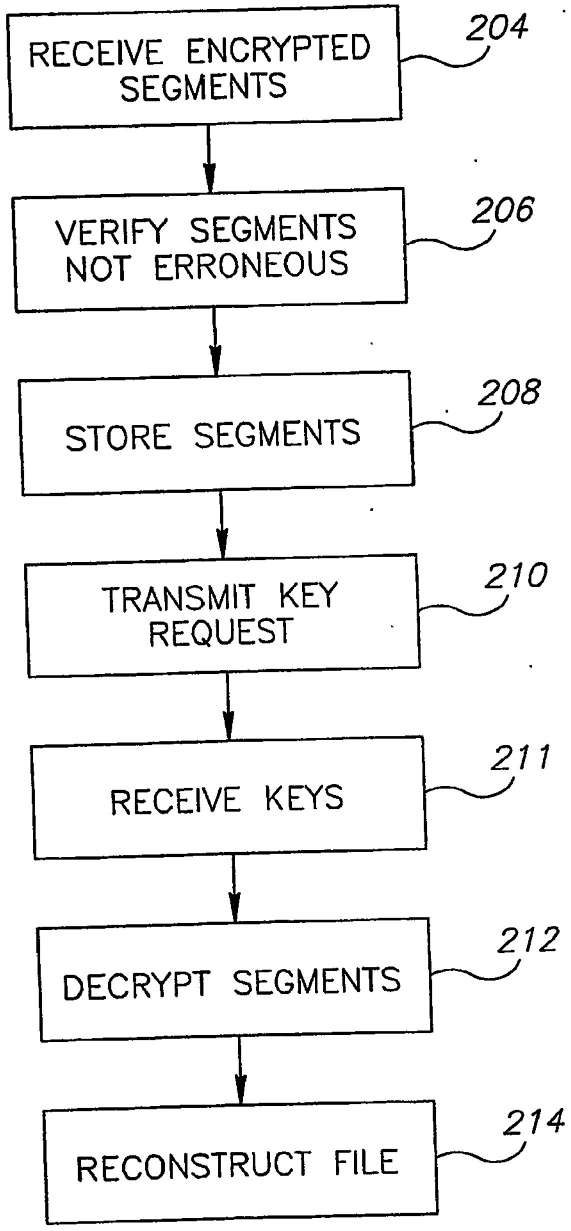
RECEIVE ENCRYPTED SEGMENTS
204
VERIFY SEGMENTS NOT ERRONEOUS
206
STORE SEGMENTS
208
TRANSMIT KEY REQUEST
210
RECEIVE KEYS
211
DECRYPT SEGMENTS
212
RECONSTRUCT FILE
214

FIG.2

IL 04/00903

מדינת ישראל
STATE OF ISRAEL

Ministry of Justice
Patent Office

משרד המשפטים
לשכת הפטנטים

This is to certify that annexed hereto is a true copy of the documents as originally deposited with the patent application particulars of which are specified on the first page of the annex.

זאת לתעודה כי רצופים בזה העתקים נכונים של המסמכים שהופקדו לכתחילה עם הבקשה לפטנט לפי הפרטים הרשומים בעמוד הראשון של הנספח.

This 17-10-2004 היום

נ. לשרי
ממונה על הבוחנים

רשם הפטנטים
Commissioner of Patents

נתאשר
Certified

PCT REQUEST

Original (for SUBMISSION)

0	For receiving Office use only	
0-1	International Application No.	PCT/IL2004/000805
0-2	International Filing Date	07 SEP 2004 (07-09.2004)
0-3	Name of receiving Office and "PCT International Application"	ISRAEL PATENT OFFICE PCT International Application

0-4	Form PCT/RO/101 PCT Request	
0-4-1	Prepared Using	PCT-SAFE [EASY mode] Version 3.50 (Build 0002.162)
0-5	Petition The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	Receiving Office (specified by the applicant)	Israel Patent Office (RO/IL)
0-7	Applicant's or agent's file reference	279/04168
I	Title of Invention	ITERATIVE FORWARD ERROR CORRECTION
II	Applicant	
II-1	This person is	applicant only
II-2	Applicant for	all designated States except US
II-4	Name	BAMBOO MEDIACASTING LTD.
II-5	Address	P. O. BOX 5035 44150 KFAR SABA Israel
II-6	State of nationality	IL
II-7	State of residence	IL
II-8	Telephone No.	+972 (9) 746 4676
II-9	Facsimile No.	+972 (9) 746 4674
III-1	Applicant and/or Inventor	
III-1-1	This person is	applicant and inventor
III-1-2	Applicant for	US only
III-1-4	Name (LAST, First)	AMRAM, Noam
III-1-5	Address	12 TCHARNIHOVSKI STREET 58382 HOLON Israel
III-1-6	State of nationality	IL
III-1-7	State of residence	IL

III-2	**Applicant and/or Inventor**	
III-2-1	This person is	applicant and inventor
III-2-2	Applicant for	US only
III-2-4	Name (LAST, First)	ENTIN, Leonid
III-2-5	Address	10 ADMONIT STREET 71700 MODIIN Israel
III-2-6	State of nationality	IL
III-2-7	State of residence	IL
IV-1	**Agent or common representative; or address for correspondence** The person identified below is hereby/ has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	agent
IV-1-1	Name (LAST, First)	FENSTER, Paul
IV-1-2	Address	FENSTER & COMPANY PATENT ATTORNEYS, LTD. P. O. BOX 10256 49002 PETACH TIKVA Israel
IV-1-3	Telephone No.	+972 3 921-5380
IV-1-4	Facsimile No.	+972 3 921-5383
IV-2	**Additional agent(s)**	additional agent(s) with same address as first named agent
IV-2-1	Name(s)	FENSTER,Maier; ENTIS,Allan; SCHATZ,Yaakov
V	**DESIGNATIONS**	
V-1	**The filing of this request constitutes under Rule 4.9(a), the designation of all Contracting States bound by the PCT on the international filing date, for the grant of every kind of protection available and, where applicable, for the grant of both regional and national patents.**	
VI-1	**Priority claim of earlier national application**	
VI-1-1	Filing date	11 September 2003 (11.09.2003)
VI-1-2	Number	157885
VI-1-3	Country	IL
VI-2	**Priority document request** The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) identified above as item(s):	VI-1

VII-1	International Searching Authority Chosen	United States Patent and Trademark Office (USPTO) (ISA/US)	
VIII	Declarations	Number of declarations	
VIII-1	Declaration as to the identity of the inventor	-	
VIII-2	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent	-	
VIII-3	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application	-	
VIII-4	Declaration of inventorship (only for the purposes of the designation of the United States of America)	-	
VIII-5	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty	-	
IX	Check list	number of sheets	electronic file(s) attached
IX-1	Request (including declaration sheets)	4	✓
IX-2	Description	18	-
IX-3	Claims	7	-
IX-4	Abstract	1	✓
IX-5	Drawings	3	-
IX-7	TOTAL	33	
	Accompanying Items	paper document(s) attached	electronic file(s) attached
IX-8	Fee calculation sheet	✓	-
IX-11	Copy of general power of attorney	✓	-
IX-17	PCT-SAFE physical media	-	✓
IX-19	Figure of the drawings which should accompany the abstract	1	
IX-20	Language of filing of the international application	English	
X-1	Signature of applicant, agent or common representative	Paul Fenster	
X-1-1	Name (LAST, First)	FENSTER, Paul	
X-1-2	Name of signatory		
X-1-3	Capacity		

FOR RECEIVING OFFICE USE ONLY

10-1	Date of actual receipt of the purported international application	07 SEP 2004 (07-09.2004)
10-2	Drawings:	
10-2-1	Received	✓
10-2-2	Not received	
10-3	Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application	
10-4	Date of timely receipt of the required corrections under PCT Article 11(2)	
10-5	International Searching Authority	ISA/US
10-6	Transmittal of search copy delayed until search fee is paid	✓

FOR INTERNATIONAL BUREAU USE ONLY

11-1	Date of receipt of the record copy by the International Bureau	

279/04168

1/1

PCT REQUEST (ANNEX - FEE CALCULATION SHEET)

Original (for SUBMISSION)

(This sheet is not part of and does not count as a sheet of the international application)

0	For receiving Office use only	
0-1	International Application No.	PCT/IL2004/000805
0-2	Date stamp of the receiving Office	07 SEP 2004 (07.09.2004)

0-4	Form PCT/RO/101 (Annex) PCT Fee Calculation Sheet			
0-4-1	Prepared Using	PCT-SAFE [EASY mode] Version 3.50 (Build 0002.162)		
0-9	Applicant's or agent's file reference	279/04168		
2	Applicant	BAMBOO MEDIACASTING LTD.		
12	Calculation of prescribed fees	fee amount/mulipier	Total amounts (ILS)	Total amounts (USD)
12-1	Transmittal fee T	⇨	476	
12-2-1	Search fee S	⇨		1000
12-2-2	International search to be carried out by	US		
12-3	International filing fee (first 30 sheets) i1	1134 USD		
12-4	Remaining sheets	3		
12-5	Additional amount (X)	12 USD		
12-6	Total additional amount i2	36 USD		
12-7	i1 + i2 = i	1170 USD		
12-12	EASY Filing reduction R	USD-81		
12-13	Total International filing fee (i-R) I	⇨		1089
12-14	Fee for priority document Number of priority documents requested	1		
12-15	Fee per document (X)	0 ILS		
12-16	Total priority document fee: P	⇨		
12-17	TOTAL FEES PAYABLE (T+S+I+P)	⇨	476	2089
12-19	Mode of payment	other Please bill us.		

PCT

Original (for SUBMISSION)

13-2-7	Validation messages Contents	Green? Reference number for attached copy of general power of attorney not indicated.

ITERATIVE FORWARD ERROR CORRECTION

FIELD OF THE INVENTION

The present invention relates generally to communication networks and particularly to method of forward error corrections.

BACKGROUND OF THE INVENTION

In transmission of data packets over packet based networks, there is a possibility of packet loss, such that it may be assumed that a certain percentage of packets are lost on any packet based network. Packets may be lost due to channel conditions and/or due to application operation, for example late tuning onto a data transmission. In some cases, such as transfer of a file, the loss of even a small percentage of the transmitted data prevents the use of the entire file.

In some cases, redundant data is transmitted along with the transmitted data, such that even if some of the transmitted data is lost, the original data can be reconstructed from the data that was received. One method of redundancy is referred to as forward error correction (FEC). In accordance with a simple FEC code, the protected data is included in a single source word (also referred to as a block), divided into a set X of k source elements (original elements). For the single source word, n > k code elements (referred to also as FEC elements), of the same size as the source elements, are generated, in order to represent the source words in a protected manner. The n code elements are referred to together as a code word. The elements may be of different sizes, such as single bits or packets. A receiver needs to receive correctly any k+z elements (z >= 0) from the transmitted code word in order to reconstruct the source word. When z=0 the code is considered optimal.

Various coding methods of generating the code elements from the source elements, are known in the art. One of the attributes of coding methods is the ratio k/n, which is referred to as the code rate. The code rate used depends on the expected data loss rate, the importance of the data and the available bandwidth.

Generally, there exist efficient coding methods only for several coding rates. When it is desired to have a code rate that does not have an efficient coding method, a method with a lower code rate (i.e., a higher n for the same k) is used to generate the code elements, and then some of the code elements are dropped. The dropped code elements are referred to as punctured elements. In some cases, punctured elements are retransmitted, instead of or in addition to other code elements not correctly received.

If the source word is a subset of the code word (i.e., X is a subset of Y), the code is referred to as a systematic code. The portion of the code word not included in the source word is referred to as a parity word. Codes in which the source word is not a subset of the code word are referred to as non-systematic codes.

When possible, it is considered advantageous to include an entire data file in a single source word, for which a single code word is generated. The available codes, however, such as the Reed Solomon (RS) code, require large processing resources when the source word is large. In order to reduce the processing power required, in one-dimensional codes (known also as single dimension codes), the original data is divided into a plurality of source words and code words are generated for each source word independently.

As the size of the original data increases, the number of source words increases, and therefore the chances of successfully reconstructing the original data decreases, since all the source words need to be reconstructed independently. Excess elements (beyond k+z) received for one of the source words does not aid in the reconstruction of other source words for which a sufficient number of elements was not received.

In an exemplary two-dimensional code, the original data is arranged in a two-dimensional array. Each row and each column of the array is viewed as a separate source word, for which a code word is generated. In the data reconstruction, the elements of each row code word which is successfully reconstructed can be used in the reconstruction of column code words and vice versa. An iterative "column-row" reconstruction method is generally used to reconstruct the data.

For substantially the same complexity (i.e., processing resources), the two-dimensional FEC requires less bandwidth than the one-dimensional FEC. For high-loss transmission links and for short original data, the two-dimensional FEC becomes inefficient.

SUMMARY OF THE INVENTION

An aspect of some embodiments of the invention relates to a multi-dimension (e.g., two dimensional) code in which parity elements are generated, in one dimension, for punctured elements, which were not transmitted, of a different dimension. Optionally, parity elements are generated for an entire row of punctured elements and only the parity elements (and not the punctured elements themselves) are transmitted. The term parity elements refers herein to the elements beyond the k elements of a code word required in order to reconstruct the source word corresponding to the code word. The parity elements may include the code elements that are not source elements, in a systematic code and/or may include arbitrary code elements in a non systematic code. During reconstruction, the punctured elements may be reconstructed, in order to reconstruct other elements within the code words.

An aspect of some embodiments of the invention relates to a code in which different numbers of parity elements are generated for different source words (e.g., rows, columns and/or blocks of data) having equivalent importance. In some embodiments of the invention, different numbers of parity elements of a second (or higher) dimension are generated for the rows and/or columns of a first (or lower) dimension. The different numbers of parity elements may include, at least 3 or even 5 different numbers of parity elements for different rows. In some embodiments of the invention, at least 10 different rows have different numbers of parity elements.

The reconstruction of rows for which more parity elements were generated will generally allow for reconstruction of one or more columns and hence provide additional elements for reconstruction of the rows for which fewer redundancy elements were generated.

An aspect of some embodiments of the invention relates to a code in which parity elements of a second dimension are generated for only some of the rows of the code elements of a first dimension, e.g., only for some of the rows of the original data and/or for only some of the rows of the redundant data. Generally, the other rows will be reconstructed using the first dimension redundancy elements, after some of the rows for which second-dimension redundancy was provided are reconstructed.

The methods of the present invention were determined to achieve a higher efficiency than one-dimensional and two-dimensional FEC schemes, especially for links having high loss rates. In addition, the efficiency of the methods of the present invention has low dependence on the size of the original data and/or the link loss rate, such that the same code may be used regardless of the expected data size and link conditions.

An aspect of some embodiments of the invention relates to concurrently transmitting FEC elements representing a data block on a plurality of channels, the channels not carrying identical sequences of FEC elements. The concurrent transmission of the FEC elements on the plurality of channels generally means that the beginning and end times of the transmission of the FEC elements of the data block on the plurality of channels overlap to a large extent. It is noted, however, that the channels may use different time slots of a time division scheme, such that although the transmissions in general are concurrent, at the time slot level the signals may not be transmitted together. Optionally, the plurality of channels transmit from a single transmitter.

In some embodiments of the invention, at least one of the receivers can tune onto all the channels concurrently. The transmission of the FEC elements on a plurality of different channels in non-identical sequences, allows reception of the data block by receivers of different capabilities from different channels, while allowing receivers listening to a large number of channels to receive the data block faster.

There is therefore provided in accordance with an exemplary embodiment of the invention, a method of preparing data for transmission, comprising providing a block of data, generating a plurality of first dimension code words including first dimension forward error correction FEC elements, the elements of each code word may be used interchangeably to reconstruct a data portion of the block corresponding to the code word, defining a plurality of second dimension source words formed of the generated elements and generating for at least two of the defined second dimension source words, different numbers of parity elements.

Optionally, at least some of the first dimension FEC elements are not included in second dimension code words for which second dimension parity elements are generated.

Optionally, generating the first dimension code words comprises generating according to a systematic code. Optionally, second dimension parity elements are generated for fewer than half the first dimension elements. Optionally, generating second dimension parity elements comprises generating such that at least five of the defined second dimension source words have different code rates. Optionally, generating second dimension parity elements comprises generating such that each second dimension source word for which parity elements are generated, has a different number of elements.

Optionally, generating second dimension parity elements comprises generating parity elements in accordance with each code rate for which parity elements are generated, for a same number of second dimension source words. Optionally, generating first dimension code words comprises generating code words including different numbers of elements.

Optionally, the method includes transmitting all the generated first and second dimension elements to a receiver. Optionally, the method includes transmitting fewer than all the generated first and second dimension elements to a receiver. Optionally, first dimension elements belonging to second dimension source words for which parity elements were generated, are not transmitted. Optionally, transmitting the data comprises transmitting over a channel having a loss rate greater than 30%. Optionally, each element comprises a data packet. Alternatively, each element comprises a single bit.

There is further provided in accordance with an exemplary embodiment of the invention, a method of transmitting data, comprising providing a block of data, generating a plurality of first dimension code words of first forward error correction FEC elements, the elements of each code word may be used interchangeably to reconstruct a data portion of the block corresponding to the code word, generating one or more second dimension code words, each second dimension code word including source elements from one or more of the first dimension code words, transmitting elements representing the data block to a receiver, the transmitted elements not including at least one element belonging to both a first and second dimension code word.

Optionally, transmitting the elements comprises transmitting all the elements of the second dimension code words that do not belong to first dimension code words. Optionally, generating the first dimension code words comprises generating code words including source elements and parity elements and wherein some of the parity elements are transmitted and some of the parity elements are not transmitted. Optionally, the source elements and the transmitted parity elements of each first dimension code word are of a number required to allow, on the average, reconstruction of between about 35-50% of the code words, without the non-transmitted parity elements, taking into account an expected loss rate during the transmission. Optionally, each first dimension code word includes a number of elements sufficient to allow, on the average, reconstruction of at least 95% of the first dimension code words based on transmission of the elements of the code words, taking into account an expected loss rate during the transmission.

Optionally, each first dimension code word includes a number of elements sufficient to allow, on the average, reconstruction of less than 98% of the first dimension code words based on transmission of the elements of the code words, taking into account an expected loss rate during the transmission. Optionally, each first dimension code word includes a number of elements sufficient to allow, on the average, reconstruction of less than 95% of the first dimension code words based on transmission of the elements of the code words, taking into account an expected loss rate during the transmission.

Optionally, more than 20% of the elements common to first and second dimension codes are not transmitted. Optionally, generating second dimension code words comprises generating a plurality of code words of different code rates. Alternatively, generating second dimension code words comprises generating a plurality of code words with same code rates.

Optionally, all the common elements of first and second dimension code words of at least one code word are not transmitted. Optionally, generating second dimension code words comprises generating at least one second dimension code word having one element from each of the first dimension code words. Optionally, the method includes generating and transmitting elements of a third dimension code word. Optionally, generating the code words comprises generating according to a block code and/or a convolution code.

Optionally, transmitting the elements comprises transmitting over a plurality of different channels. Optionally, transmitting the elements comprises transmitting over a plurality of channels with different expected loss rates. Optionally, elements belonging to second dimension code words but not to the first dimension code word are transmitted on a separate channel from elements of first dimension code words. Optionally, elements belonging to second dimension code words but not to the first dimension code words are transmitted on a channel having a lower loss rate than a channel used for elements of first dimension code words.

There is further provided in accordance with an exemplary embodiment of the invention, a method of transmitting data, comprising providing a block of data, generating a plurality of FEC elements of one or more dimensions that represent the block of data, and transmitting the plurality of FEC segments over a plurality of different channels.

Optionally, generating the plurality of FEC elements comprises generating elements according to a single dimension FEC method. Alternatively, generating the plurality of FEC elements comprises generating elements according to a multi-dimension FEC method. Optionally, transmitting the plurality of FEC segments comprises transmitting all elements belonging to a same code word on a single channel. Alternatively, transmitting the plurality of FEC segments comprises transmitting elements belonging to at least one single code word on a plurality of channels.

Optionally, transmitting the plurality of FEC segments comprises transmitting on a plurality of channels having same or different loss rates. Optionally, transmitting the plurality of FEC segments comprises transmitting on a plurality of channels having different loss rates due to different transmission methods. Optionally, transmitting the plurality of FEC segments comprises transmitting only systematic FEC elements on at least one of the channels. Optionally, the method includes receiving the transmitted plurality of segments by a plurality of receivers, at least one of the receivers receives segments on fewer than all the channels on which the FEC segments are transmitted.

Optionally, generating the FEC elements comprises generating code words of one or more first dimensions and parity elements of one or more second dimensions and wherein transmitting the plurality of FEC segments comprises transmitting such that one or more channels do not carry the parity elements of the one or more second dimensions. Optionally, one or more channels carry only the parity elements of the one or more second dimensions. Optionally, the method includes receiving the transmitted plurality of segments by a plurality of receivers, at least one of the receivers receives segments on fewer than all the channels on which the FEC segments are transmitted.

Optionally, the method includes receiving the transmitted plurality of segments by a plurality of receivers, at least one of the receivers having the capability to listen concurrently to all the channels and at least one of the receivers not having the capability to listen concurrently to all the channels. Optionally, the sequences of elements of different channels differ in at least some of the elements they contain. Optionally, the sequences of elements of at least two channels include the same elements in different orders. Optionally, the sequences of elements of at least two channels do not include any common elements.

There is further provided in accordance with an exemplary embodiment of the invention, a method of receiving data, comprising tuning onto a plurality of channels, receiving FEC elements on each of the plurality of channels and reconstructing a data block using one or more FEC elements received over each of the plurality of channels.

Optionally, the plurality of channels include at least two channels having different loss rates. Optionally, receiving the FEC elements comprises receiving only parity elements on at least one of the channels. Optionally, receiving the FEC elements comprises receiving only systematic elements on at least one of the channels. Optionally, receiving the FEC elements comprises receiving elements of a single code word on at least two different channels.

There is further provided in accordance with an exemplary embodiment of the invention, a multicast transmission unit, comprising an input interface for receiving blocks of data, a processor adapted to generate a plurality of first dimension code words including first dimension forward error correction FEC elements, the first dimension elements of each code word may be used interchangeably to reconstruct a data portion of the block corresponding to the code word, to define a plurality of second dimension source words formed of the generated first dimension FEC elements and to generate for at least two of the defined second dimension source words, different numbers of parity elements and a transmitter for transmitting FEC elements generated by the processor.

Optionally, the transmitter is adapted to transmit FEC elements generated by the processor for a single block on a plurality of channels.

BRIEF DESCRIPTION OF FIGURES

Particular non-limiting embodiments of the invention will be described with reference to the following description of non-limiting exemplary embodiments in conjunction with the figures. Identical structures, elements or parts which appear in more than one figure are preferably labeled with a same or similar number in all the figures in which they appear, in which:

Fig. 1 is a schematic illustration of a forward error correction (FEC) code construction, in accordance with an exemplary embodiment of the invention;

Fig. 2 is a flowchart of acts performed by the receiver in reconstructing the original data, in accordance with an exemplary embodiment of the invention; and

Fig. 3 is a schematic illustration of a code construction, in accordance with another exemplary embodiment of the invention.

DETAILED DESCRIPTION OF EMBODIMENTS

Consider the situation where a transmitter is to transmit original data over a lossy channel to a receiver. In order to allow reconstruction of the transmitted data by the receiver, the transmitter generates FEC code elements, which are transmitted to the receiver.

Fig. 1 is a schematic illustration of a forward error correction (FEC) element arrangement, in accordance with an exemplary embodiment of the invention. The original data is optionally divided into blocks of a predetermined size, each block is handled separately as is now described with reference to Fig. 1, which shows a single block 100. The size of block 100 is optionally selected according to the processing resources of the receivers that need to reconstruct the data.

Block 100 is divided into a plurality (e.g., 1000) of source elements 102 organized in first-dimensional (column) source words 104. In the example of Fig. 1, ten column source words 104, each including one hundred source elements 102, are constructed for each block 100. For each column source word 104, parity elements 106 are generated in accordance with a systematic code. The column source word 104 together with the parity elements 106 form a column code word 122. The parity elements 106 of each column code word 122 are optionally divided into a first parity sub-word 108 and a second parity sub-word 110. The parity elements 106 of the first parity sub-words 108 are optionally transmitted to the receiver, while the parity elements 106 of the second parity sub-words 110 are not transmitted to the receiver.

In the example of Fig. 1, each source word 102 includes 100 elements, each first parity sub-word 108 includes 30 elements and each second parity sub-word 110 includes 20 elements. In this example, 60% of the parity elements 106 belong to first parity sub-words 108, while 40% of the parity elements 106 belong to second parity words 110. Naturally, other percentages may be used. Particular expected values range between about 55-75% of parity elements 106 belonging to first parity sub-words 106, although other ranges (e.g., 30-50%) may also be useful.

Parity elements 106 are optionally generated using any suitable FEC code method known in the art. In some embodiments of the invention, a convolution code is used to generate the parity elements. Alternatively or additionally, the elements are generated using a block code. In some embodiments of the invention, the elements are generated using both convolution and block codes, some code words using one FEC code method while other code words use another FEC code method. Optionally, code words of different dimensions use different FEC methods (e.g., block and convolution). Alternatively or additionally, different code words of the same dimension use different FEC methods.

The non-transmitted parity elements 106 of sub-words 110 are optionally included in second-dimension (row) source words 114. In some embodiments of the invention, for each row word 114, a second-dimension row parity word 116 of second dimension parity elements 112 is generated. These second dimension parity elements 112 are transmitted to the receiver in order to aid in reconstruction of the original data. Row source words 114 and their respective row parity words 116 are referred to together as row code words 118. In some embodiments of the invention, the elements of row source words 114 are first dimension parity elements, while in the second dimension they serve as source elements.

The transmission of row parity words 116 instead of row source words 114 increases the efficiency of the code. This is especially true for a transmission with large expected variations in the total number of source elements 102 and parity elements 106 received for different code words 122. The reception of additional elements 102 and/or 106 from row source words 114 would be redundant for column code words 122 that have sufficient elements without the elements of row source words 114, and would not aid the reconstruction of other columns, as the columns are not inter-related. The elements of row parity words 116, on the other hand, can be used for reconstructing any of the column source words 104.

The generation of parity words 116 only for some of the first dimension parity elements 106, i.e., for the parity elements 106 of the second parity words 110, reduces the amount of data transmitted over the channel, while achieving the benefits of the invention. Optionally, the parity elements 106 for which second dimensional row parity words 116 are generated, are selected arbitrarily and/or randomly, without relation to their contents. Furthermore, alternatively to generating second dimensional parity words 116 for first dimension parity elements 106, the second dimensional parity words 116 may be generated for one or more rows of source elements 102. Optionally, in this alternative, the rows of source elements 102 for which second dimension parity rows 116 are generated, are not transmitted.

In some embodiments of the invention, the number of parity elements 106 in the first parity sub-word 108 is selected according to the expected loss rate of the channel, so that the number of column source words 104 which may be reconstructed by the receiver using only the received source elements 102 and the received parity elements 106 of the first parity sub-words 108, is about a desired percentage. In an exemplary embodiment of the invention, the desired percentage is between about 35-50%, e.g., 40%. The desired percentage is optionally selected as a low enough percentage to prevent there being too many columns receiving many more elements than required for reconstruction, while ensuring easy reconstruction of row source words 114 without transmitting too many second dimension parity elements 112.

The number of parity elements 106 in second parity sub-words 110 is optionally selected according to the loss rate of the channel, such that the number of column source words 104 which can be reconstructed by the receiver using the received elements, if source elements 102 are transmitted with all the parity elements 106 (of both the first and second parity sub-words 108 and 110) but no row parity elements 112 are transmitted, is between about 95-100%.

The number of second dimensional parity elements 112 generated is optionally selected so that the row source words 114 can be reconstructed given the loss rate of the channel and the number of column code words 122 which are expected to be reconstructed without the second dimensional parity elements 112.

Alternatively to generating the same number of second dimension parity elements 112 for all the row source words 114, different numbers of second dimensional parity elements 112 are generated for different row source words 114. Stated otherwise, the second dimension code has different code rates for different row source words 114. Optionally, the numbers of second dimensional parity elements 112 generated for different row source words 114 span over a large range of numbers, for example between 1 and a maximal number of elements 112 generated for a row source word 114. In some embodiments of the invention, the numbers of second dimensional elements 112 generated for different row source words 114 is distributed evenly over the range from which the number of elements is taken. Alternatively or additionally, the row source words 114 are divided into substantially same size groups, and each group has a different number of second dimension parity elements 112.

In some embodiments of the invention, the second dimensional parity elements 112 are organized in a triangle with decreasing numbers of elements 112 in each row parity word 116. For example, when there are twenty row source words 114, a first row parity word 116 has twenty second dimensional parity elements 112, a second row parity word 116 has nineteen parity elements 112 and so on until a last row parity word 116 has only a single parity element 112. The use of decreasing numbers of elements is found to be efficient since after reconstruction of one row source word 114, more column source words 104 are expected to be reconstructed and therefore other row source words 114 will be reconstructable using fewer second dimensional parity elements 112. This process repeats until all the original column source words 104 are reconstructed.

Alternatively to using an isosceles triangle of parity elements 112, any other triangular or non-triangular arrangement of elements in parity words 116 may be used, for example based on simulations of the expected reconstruction possibilities. For example, second dimensional redundancy elements 112 are optionally organized in a non-isosceles triangle, a trapezoid, a concave or a convex structure which maximizes the efficiency of the code.

In some embodiments of the invention, the structure of the code (e.g., the number of columns and/or rows) and other details of the FEC method are preconfigured in both the transmitter and the receiver. Alternatively, the code structure details are transmitted at the beginning of the transmission and/or periodically to the receiver.

The second dimension source words 114 are described above as including first dimension parity elements 106. In other embodiments of the invention, the second dimension source words 114 include first dimension source elements 102 or some second dimension source words 114 including first dimension source elements 102 and other second dimension source words 114 include first dimension parity elements 106.

Fig. 2 is a flowchart of acts performed by the receiver in reconstructing the original data, in accordance with an exemplary embodiment of the invention. The elements actually received (202), i.e., detected and utilized by the receiver, are de-interleaved (organized) (204) in the format of Fig. 1, generally based on identification headers included in the elements. If (205) additional elements are required for reconstruction, and the transmission was not completed (207), the receiver continues to receive (202) more elements. If the transmission was completed, without the receiver accumulating a group of elements required to reconstruct the data block, the reconstruction failed (222). The receiver may request supplementary transmission of additional elements or may request retransmission of the entire data block. If (205) additional elements are not required, iterative reconstruction of the data block is performed, as is now described.

For each column code word 104 for which the receiver has a sufficient number of elements 102 and/or 106, the receiver reconstructs (206) the column source word 104. Thereafter, the parity elements 106 of the column code word 122 are reconstructed (208). It is noted that the reconstruction (206) of the source elements 102 is not performed based on parity elements 106 of the second parity sub-word 110 since they are not transmitted at all. On the other hand, the generation (208) of the parity elements 106 includes elements of both the first parity sub-words 108 and second parity sub-words 110.

For each row code word 118 for which the receiver has a sufficient number of elements (including both first dimension parity elements 106 and second dimension parity elements 112), the receiver reconstructs (210) the parity elements 106 of row source words 114. Thereafter, the receiver repeats the reconstructing (206) of the column source words 104 that have sufficient elements for reconstructing, in view of the reconstruction performed on row code words 118. The first dimension generation (208) of parity elements 106, the second dimension reconstruction (210) of parity elements 106 and the reconstruction (206) of source elements 102 are repeated until the data block is reconstructed or no additional row or column code words were reconstructed.

Referring in more detail to determining (205) whether additional elements are required, in some embodiments of the invention, based on the number of elements in each column source word 104, the receiver determines which column source words 104 can be reconstructed. Thereafter, based on the number of elements received or reconstructed successfully from each row code word 118, the receiver determines which row code words 118 can be reconstructed. According to the results, the receiver optionally determines which column source words 104 can be reconstructed. This procedure is optionally repeated iteratively until it is determined whether or not the block can be reconstructed. Alternatively to performing exact simulations, the question of whether additional elements are required is determined based on an estimation. Optionally, in this alternative, a safety margin is taken in order to ensure that when it is determined that additional elements are not required, the chances that the reconstruction will not succeed is close to zero. In an exemplary embodiment of the invention, the estimation of whether additional elements are required is based on the number of elements received. The required number is optionally sufficiently high, such that the chances of reconstructing the data block are sufficiently high.

In some embodiments of the invention, as shown in the reconstruction method of Fig. 2, the reconstruction is performed after all the transmitted data is received. Thus, the processing resources used for the reconstruction are kept low. Alternatively, the reconstruction is attempted after a predetermined number of elements are successfully received, while additional data is being received on the channel.

In some embodiments of the invention, for example in a multicast channel, the transmission is continued for a predetermined time which is expected to be sufficient for all or nearly all receivers to receive the data. In an exemplary embodiment of the invention, the transmission has a duration of 3-4 times that required for transmission of the data on a lossless channel. Alternatively or additionally, the transmission is terminated responsive to acknowledgement that the data was received by a predetermined number of receivers (in a unicast channel, by the receiver).

Alternatively to the receiver listening to the channel until the data is completely reconstructed, the receiver listens to the channel for a predetermined time and/or until a predetermined number of elements are accumulated. The receiver then stops listening to the channel until the initial reconstruction process is completed or is performed for a predetermined number of rounds. According to the results of the initial reconstruction and optionally the time remaining for which the data will still be transmitted, the receiver then listens to the channel for an additional period. The reconstruction is continued using the data from the additional listening to the channel. This alternative is especially useful when the processing power required for signal reception is greater than required for reconstuction of the original data.

The present invention may be employed on substantially any transmitter, receiver and/or channel including wireless LAN, cellular, packet based, ATM and satellite networks. The present invention is especially useful for high loss networks, such as for data passing on noisy channels with a loss rate of above 10% or even above 30%. The high loss may also be due to the receiver listening to only a portion of the transmitted data, for example due to a late tuning on to the channel. Such late tuning may especially occur on a multicast channel, when a plurality of different receivers want to receive the same data and therefore all need to tune on to the same channel.

In an exemplary embodiment of the invention, the present invention is used for transmission of data to a plurality of wireless receivers on a multicast channel. Optionally, the data is transmitted after encoding with a code having a code rate between about 0.2-0.4, such that data which requires 2 minutes for uncoded transmission requires between 5-10 minutes for coded transmission. Such a redundancy corresponds to a loss rate of about 70-80%.

In some embodiments of the invention, in addition to first dimension parity elements 106 and second-dimension redundancy elements 112, the transmitter may generate and/or transmit additional elements, such as second dimensional FEC elements on source elements 102 and/or third dimensional code elements. In some embodiments of the invention, second-dimensional redundancy elements 112 are transmitted with a higher protection rate than source elements 102 and/or on a separate channel having a lower average loss rate. In these embodiments, the size of first parity sub-words 108 is optionally reduced accordingly, taking into account the increased reliability of the second-dimensional redundancy elements 112.

Although in the above description the parity elements 106 which were generated but not transmitted belong to the first dimension, the same principal may be used for any other dimension, such as second or third dimension parity or source elements. The elements which were generated but not transmitted may belong to a single code word or to a plurality of code words in a plurality of dimensions.

Fig. 3 is a schematic illustration of a forward error correction (FEC) element construction, in accordance with another exemplary embodiment of the invention. A block of original data is divided into source elements 102, organized in a two dimension array of column source words 104 and row source words 128. For each column source word 104, first-dimension parity elements 106 are generated, with optionally different numbers of parity elements 106 being generated for different column source words 104. For each row source word 128, second dimension row parity elements 112 are generated. Optionally, also in generating row parity elements 112, different numbers of elements are generated for different row source words 128. In some embodiments of the invention, second-dimension parity elements 112 are generated only for source elements 102. Alternatively, second dimensional parity elements 112 are generated also for first dimension parity elements 106.

In some embodiments of the invention, a maximal number and a minimal number of second dimension elements 112 are provided. The number of parity elements 112 for each row source word 128 is optionally selected so as to have a gradually decreasing number of parity elements 112 from the maximal number to the minimal number along the row source words 128. Alternatively, several predetermined code rates are defined for the number of second dimension row code words. For example, each row source word 128 may optionally have one of three possible numbers of second dimension parity elements 112, corresponding to a low protection level, a medium protection level and a high protection level.

In some embodiments of the invention, all the source elements 102, first dimension parity elements 106 and second dimension parity elements 112 are transmitted to the receiver. Alternatively, some of the source elements, for example from the source elements which are most protected, are not transmitted. Generally, rows and/or columns for which fewer elements were received will be reconstructed based on reconstructed elements of other columns and/or rows.

Alternatively to having different numbers of parity elements both for different columns and for different rows, the use of different numbers of elements may be used only for different rows or only for different columns.

Optionally, the source elements 102 of different row and/or column code words have the same importance. The use of different codes for different code words is used herein based on statistical assumptions and is optionally not related to attempts to protect data portions of different importance using different code rates. In some embodiments of the invention, a scheme which incorporates different code rates for statistical purposes and uses different code rates for data of different importance is used.

In simulations performed on a channel having a loss rate of 30%, the one dimensional FEC method was determined to have an 86% efficiency, the second dimensional FEC was determined to have a 93% efficiency and a method in accordance with the present invention was found to have an efficiency of 96%. The simulations in accordance with the present invention were performed using 20 first dimension column code words having X =172 source elements and Y = 172+48 code elements. Second dimension parity elements 112 were generated for 22 rows, each having a different number of parity elements 112 between 1 to 22.

As mentioned above, in some cases different elements are transmitted on different channels with different protection levels. In some embodiments of the invention, second dimension parity elements 112 are transmitted on a channel with a higher protection level, due to their general nature which can aid in decoding many first dimension code words. Alternatively or additionally, data known to have more importance in a higher protocol layer is transmitted on a channel with a higher protection level, for example as described in PCT application PCT/IL2004/000204, titled "Segmented Data Delivery Over Non-Reliable Link", filed March 3, 2004, the disclosure of which is incorporated herein by reference.

The use of a plurality of different channels for transmission of the elements of a single block may be advantageous for other reasons than providing higher level protection to specific elements. In some embodiments of the invention, some of the elements of each first dimension code word are transmitted on a first channel, while other elements of the first dimension code words are transmitted on a second channel. Optionally, in these embodiments, the percentage of elements transmitted on the different channels is different for different first dimensional code words. The use of different channels varies the number of elements received for different code words and hence allows for an increase in the chances that the second parity elements 112 are effective for reconstruction of first dimensional code words.

In some embodiments of the invention, the use of the plurality of channels is an attribute of the transmission system used. Instead of using different channels for different data blocks, the FEC elements of at least one of the data blocks are transmitted on a plurality of channels. In some cases, different receivers have different tuning capabilities. Some receivers, for example, can listen only to a first group of channels, e.g., including 1 channel, while other receivers, can listen to a second group of channels greater than the first group, e.g., including 2 channels. In another example, some receivers listen to at most six channels while other receivers listen to nine or more channels. The number of channels is not relevant to the invention and the advantages of dividing the FEC elements of a single block to a plurality of channels pertains to substantially any number of channels.

In some embodiments of the invention, a first group of receivers is capable of tuning onto a first set of one or more channels and a second group of receivers is capable of tuning onto a second set of channels not including any channels of the first set. A third set of receivers is capable of tuning onto the channels of the first set and of the second set, or on sub-sets of the channels of both the first and second sets. Preferably, each of the sets of channels carries a sufficient number of elements required for decoding the corresponding data block. In some embodiments of the invention, during transmission of the FEC elements, the first and second channels carry sets of elements which are at least partially different, so that receivers listening to both the first and second sets of channels do not receive the same elements twice and hence receive a number of elements required for decoding faster than if they would listen only to a single set of channels. Alternatively or additionally, both sets of channels carry the same FEC elements but in a different order, so that a receiver listening to both channels will receive different elements on the channels to which it is tuned.

It is noted that the advantages of dividing the FEC segments of a single data block between a plurality of channels, are not limited to the above described multi-dimensional FEC scheme, and the division of segments may be used with substantially any FEC scheme, including a simple one dimensional FEC scheme. For example, a first number of FEC segments of each code word may be transmitted on a channel or channels to which all receivers are tuned, while additional FEC segments of each code word are transmitted on an additional channel to which only some receivers are tuned. Thus, receivers tuned to the additional channel generally receive the data blocks within a shorter period. In some embodiments of the invention, when a multi-dimensional FEC is used, the segments of code words of a first dimension are transmitted on channels to which all the receivers are tuned, while parity elements of one or more other dimensions are transmitted on a second channel.

In other embodiments of the invention, the segments of different code words of a same data block are transmitted on different channels. In these embodiments, all the receivers are optionally expected to listen to both channels. The distribution of the code words between two (or more) channels reduces the time required in order to receive each block, allowing faster decoding and utilization, e.g., display, of the data block.

In some embodiments of the invention, some of the receivers do not support FEC at all, while other receivers support using FEC. Optionally, a first channel directed to all receivers carries the systematic segments, while a second channel to which only some receivers are tuned, carries parity elements. The first channel may have a very low loss rate and/or may carry a plurality of instances of the systematic segments.

The channels used to carry the parity elements of a single data block optionally differ in their frequencies and/or codes. Alternatively or additionally, the channels differ in their time schemes and/or are transmitted from different transmitters, for example using a multi-input multi-output (MIMO) scheme. In some embodiments of the invention, the different channels have the same loss rate. Alternatively, some or all of the channels have different loss rates, for example due to different noise conditions and/or different encoding methods.

The above described methods may be used for source and parity elements 102 and 106 of different sizes, including elements which are packets and elements which are single bits. The term code element refers herein to any element which can be used to reconstruct the original data, whether the element is a source element or a parity element and/or whether the element belongs to a systematic or non-systematic code word.

The references to first and second dimensions are used herein for simplicity and the present invention may be used on codes of any number of dimensions, on some or all of the dimensions thereof. The terms first and second dimensions appearing in the claims may refer to any two of the dimensions of the code, including the first two dimensions and the last two dimensions.

It will be appreciated that the above described methods may be varied in many ways, including, changing the order of steps, and the exact implementation used. The methods of the present invention may be performed in various protocol layers and may be performed for a single transmission system in a plurality of communication protocol layers. It should also be appreciated that the above described description of methods and apparatus are to be interpreted as including apparatus for carrying out the methods and methods of using the apparatus.

The present invention has been described using non-limiting detailed descriptions of embodiments thereof that are provided by way of example and are not intended to limit the scope of the invention. For example, although the above description relates to a systematic FEC, the methods of the invention may be employed similarly on non-systematic FEC methods. It should be understood that features and/or steps described with respect to one embodiment may be used with other embodiments and that not all embodiments of the invention have all of the features and/or steps shown in a particular figure or described with respect to one of the embodiments. Variations of embodiments described will occur to persons of the art.

It is noted that some of the above described embodiments may describe the best mode contemplated by the inventors and therefore may include structure, acts or details of structures and acts that may not be essential to the invention and which are described as examples. Structure and acts described herein are replaceable by equivalents which perform the same function, even if the structure or acts are different, as known in the art. Therefore, the scope of the invention is limited only by the elements and limitations as used in the claims. When used in the following claims, the terms "comprise", "include", "have" and their conjugates mean "including but not limited to".

CLAIMS

1. A method of preparing data for transmission, comprising:

providing a block of data;

arranging the data in at least a two-dimensional array;

generating a plurality of first dimension code words including first dimension forward error correction FEC elements, the first dimension elements of each code word may be used interchangeably to reconstruct a data portion of the block corresponding to the code word;

defining a plurality of second dimension source words formed of the generated first dimension FEC elements; and

generating for at least two of the defined second dimension source words, different numbers of parity elements.

2. A method according to claim 1, wherein at least some of the first dimension FEC elements are not included in second dimension code words for which second dimension parity elements are generated.

3. A method according to claim 1, wherein generating the first dimension code words comprises generating according to a systematic code.

4. A method according to claim 1, wherein second dimension parity elements are generated for fewer than half the first dimension elements.

5. A method according to claim 1, wherein generating second dimension parity elements comprises generating such that at least five of the defined second dimension source words have different code rates.

6. A method according to claim 1, wherein generating second dimension parity elements comprises generating such that each second dimension source word for which parity elements are generated, has a different number of elements.

7. A method according to claim 1, wherein generating second dimension parity elements comprises generating parity elements in accordance with each code rate for which parity elements are generated, for a same number of second dimension source words.

8. A method according to claim 1, wherein generating first dimension code words comprises generating code words including different numbers of elements.

9. A method according to claim 1, comprising transmitting all the generated first and second dimension elements to a receiver.

10. A method according to claim 1, comprising transmitting fewer than all the generated first and second dimension elements to a receiver.

11. A method according to claim 10, wherein first dimension elements belonging to second dimension source words for which parity elements were generated, are not transmitted.

12. A method according to claim 1, wherein transmitting the data comprises transmitting over a channel having a loss rate greater than 30%.

13. A method of according to claim 1, wherein each element comprises a data packet.

14. A method of according to claim 1, wherein each element comprises a single bit.

15. A method of transmitting data, comprising:

providing a block of data;

arranging the data in at least a two-dimensional array;

generating a plurality of first dimension code words of forward error correction FEC elements, the FEC elements of each code word may be used interchangeably to reconstruct a data portion of the block corresponding to the code word;

generating one or more second dimension code words, each second dimension code word including FEC elements from one or more of the first dimension code words;

transmitting FEC elements representing the data block to a receiver, the transmitted elements not including at least one FEC element belonging to both a first and second dimension code word.

16. A method according to claim 15, wherein transmitting the elements comprises transmitting all the elements of the second dimension code words that do not belong to first dimension code words.

17. A method according to claim 15, wherein generating the first dimension code words comprises generating code words including source elements and parity elements and wherein some of the parity elements are transmitted and some of the parity elements are not transmitted.

18. A method according to claim 17, wherein the source elements and the transmitted parity elements of each first dimension code word are of a number required to allow, on the average, reconstruction of between about 35-50% of the code words, without the non-transmitted parity elements, taking into account an expected loss rate during the transmission.

19. A method according to claim 15, wherein each first dimension code word includes a number of elements sufficient to allow, on the average, reconstruction of at least 95% of the first dimension code words based on transmission of the elements of the code words, taking into account an expected loss rate during the transmission.

20. A method according to claim 15, wherein each first dimension code word includes a number of elements sufficient to allow, on the average, reconstruction of less than 98% of the first dimension code words based on transmission of the elements of the code words, taking into account an expected loss rate during the transmission.

21. A method according to claim 20, wherein each first dimension code word includes a number of elements sufficient to allow, on the average, reconstruction of less than 95% of the first dimension code words based on transmission of the elements of the code words, taking into account an expected loss rate during the transmission.

22. A method according to claim 15, wherein more than 20% of the elements common to first and second dimension code words are not transmitted.

23. A method according to claim 15, wherein generating second dimension code words comprises generating a plurality of code words of different code rates.

24. A method according to claim 15, wherein generating second dimension code words comprises generating a plurality of code words with same code rates.

25. A method according to claim 15, wherein all the common elements of first and second dimension code words of at least one code word are not transmitted.

26. A method according to claim 15, wherein generating second dimension code words comprises generating at least one second dimension code word having one element from each of the first dimension code words.

27. A method according to claim 15, comprising generating and transmitting elements of a third dimension code word.

28. A method according to claim 15, wherein generating the code words comprises generating according to a block code.

29. A method according to claim 15, wherein generating the code words comprises generating according to a convolution code.

30. A method according to claim 15, wherein transmitting the elements comprises transmitting over a plurality of different channels.

31. A method according to claim 30, wherein transmitting the elements comprises transmitting over a plurality of channels with different expected loss rates.

32. A method according to claim 30, wherein elements belonging to second dimension code words but not to the first dimension code word are transmitted on a separate channel from elements of first dimension code words.

33. A method according to claim 32, wherein elements belonging to second dimension code words but not to the first dimension code words are transmitted on a channel having a lower loss rate than a channel used for elements of first dimension code words.

34. A method of transmitting data, comprising:

providing a block of data;

generating a plurality of FEC elements of one or more dimensions that represent the block of data; and

transmitting the plurality of FEC segments over a plurality of different channels concurrently, the channels carrying sequences of elements that are not identical.

35. A method according to claim 34, wherein generating the plurality of FEC elements comprises generating elements according to a single dimension FEC method.

36. A method according to claim 34, wherein generating the plurality of FEC elements comprises generating elements according to a multi-dimension FEC method.

37. A method according to claim 34, wherein transmitting the plurality of FEC segments comprises transmitting all elements belonging to a same code word on a single channel.

38. A method according to claim 34, wherein transmitting the plurality of FEC segments comprises transmitting elements belonging to at least one single code word on a plurality of channels.

39. A method according to claim 34, wherein transmitting the plurality of FEC segments comprises transmitting on a plurality of channels having same loss rates.

40. A method according to claim 34, wherein transmitting the plurality of FEC segments comprises transmitting on a plurality of channels having different loss rates.

41. A method according to claim 40, wherein transmitting the plurality of FEC segments comprises transmitting on a plurality of channels having different loss rates due to different transmission methods.

42. A method according to claim 34, wherein transmitting the plurality of FEC segments comprises transmitting only systematic FEC elements on at least one of the channels.

43. A method according to claim 34, wherein generating the FEC elements comprises generating code words of one or more first dimensions and parity elements of one or more second dimensions and wherein transmitting the plurality of FEC segments comprises transmitting such that one or more channels do not carry the parity elements of the one or more second dimensions.

44. A method according to claim 43, wherein one or more channels carry only the parity elements of the one or more second dimensions.

45. A method according to any of claims 34-44, comprising receiving the transmitted plurality of segments by a plurality of receivers, at least one of the receivers receives segments on fewer than all the channels on which the FEC segments are transmitted.

46. A method according to any of claims 34-44, comprising receiving the transmitted plurality of segments by a plurality of receivers, at least one of the receivers having the capability to listen concurrently to all the channels and at least one of the receivers not having the capability to listen concurrently to all the channels.

47. A method according to any of claims 34-44, wherein the sequences of elements of different channels differ in at least some of the elements they contain.

48. A method according to claim 47, wherein the sequences of elements of at least two channels do not include any common elements.

49. A method according to any of claims 34-44, wherein the sequences of elements of at least two channels include at least 50% elements in common but in different orders.

50. A method of receiving data, comprising:

tuning onto a plurality of channels;

receiving FEC elements on each of the plurality of channels; and

reconstructing a data block using one or more FEC elements received over each of the plurality of channels.

51. A method according to claim 50, wherein the plurality of channels include at least two channels having different loss rates.

52. A method according to claim 50, wherein receiving the FEC elements comprises receiving only parity elements on at least one of the channels.

53. A method according to claim 50, wherein receiving the FEC elements comprises receiving only systematic elements on at least one of the channels.

54. A method according to claim 50, wherein receiving the FEC elements comprises receiving elements of a single code word on at least two different channels.

55. A multicast transmission unit, comprising:

an input interface for receiving blocks of data;

a processor adapted to generate a plurality of first dimension code words including first dimension forward error correction FEC elements, the first dimension elements of each code word may be used interchangeably to reconstruct a data portion of the block corresponding to the code word, to define a plurality of second dimension source words formed of the generated first dimension FEC elements and to generate for at least two of the defined second dimension source words, different numbers of parity elements; and

a transmitter for transmitting FEC elements generated by the processor.

56. A transmission unit according to claim 55, wherein the transmitter is adapted to transmit FEC elements generated by the processor for a single block on a plurality of channels.

ABSTRACT

A method of preparing data for transmission. The method includes providing a block of data, generating a plurality of first dimension code words including first dimension forward error correction FEC elements, the elements of each code word may be used interchangeably to reconstruct a data portion of the block corresponding to the code word, defining a plurality of second dimension source words formed of the generated elements and generating for at least two of the defined second dimension source words, different numbers of parity elements.

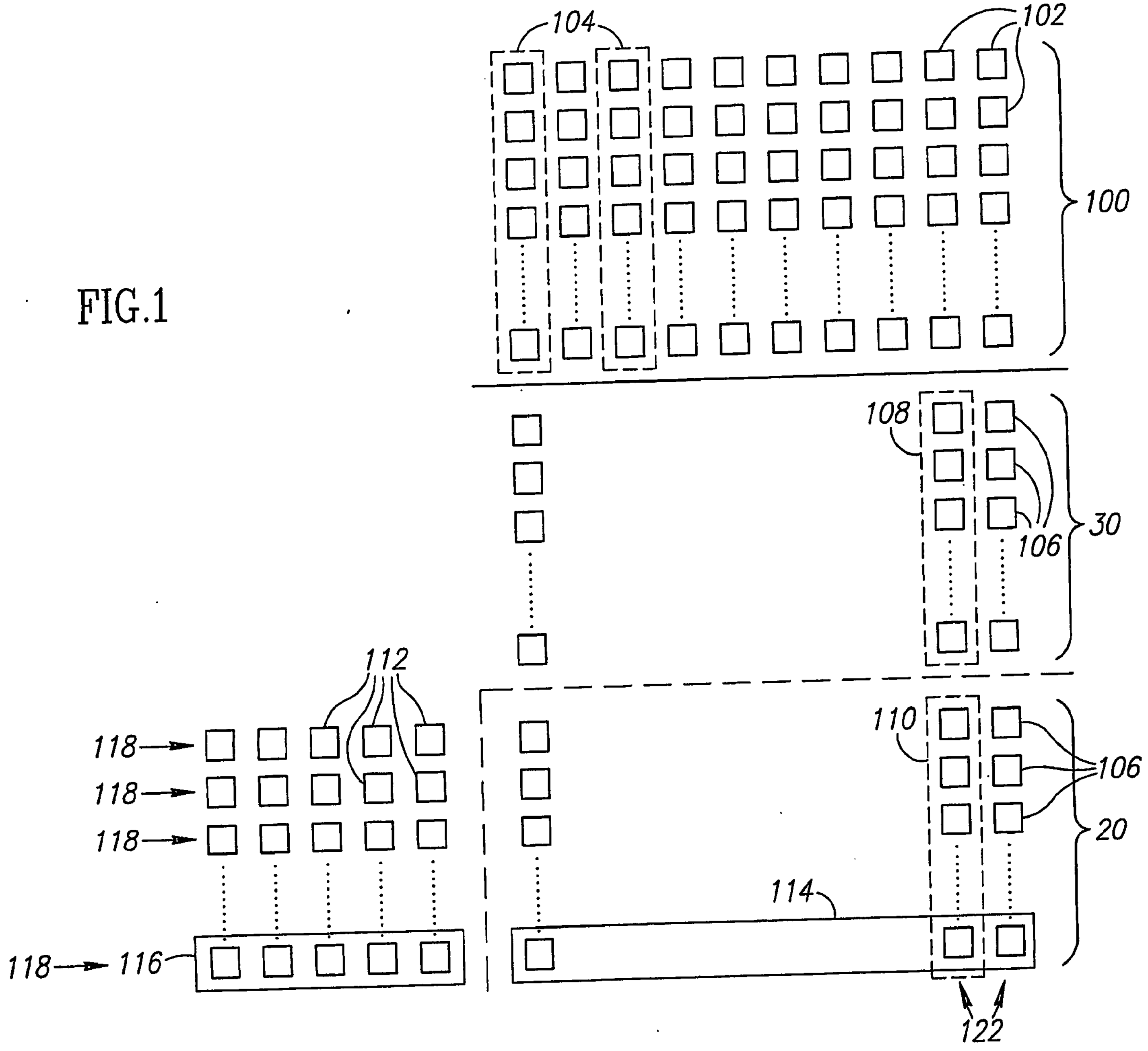

FIG.1

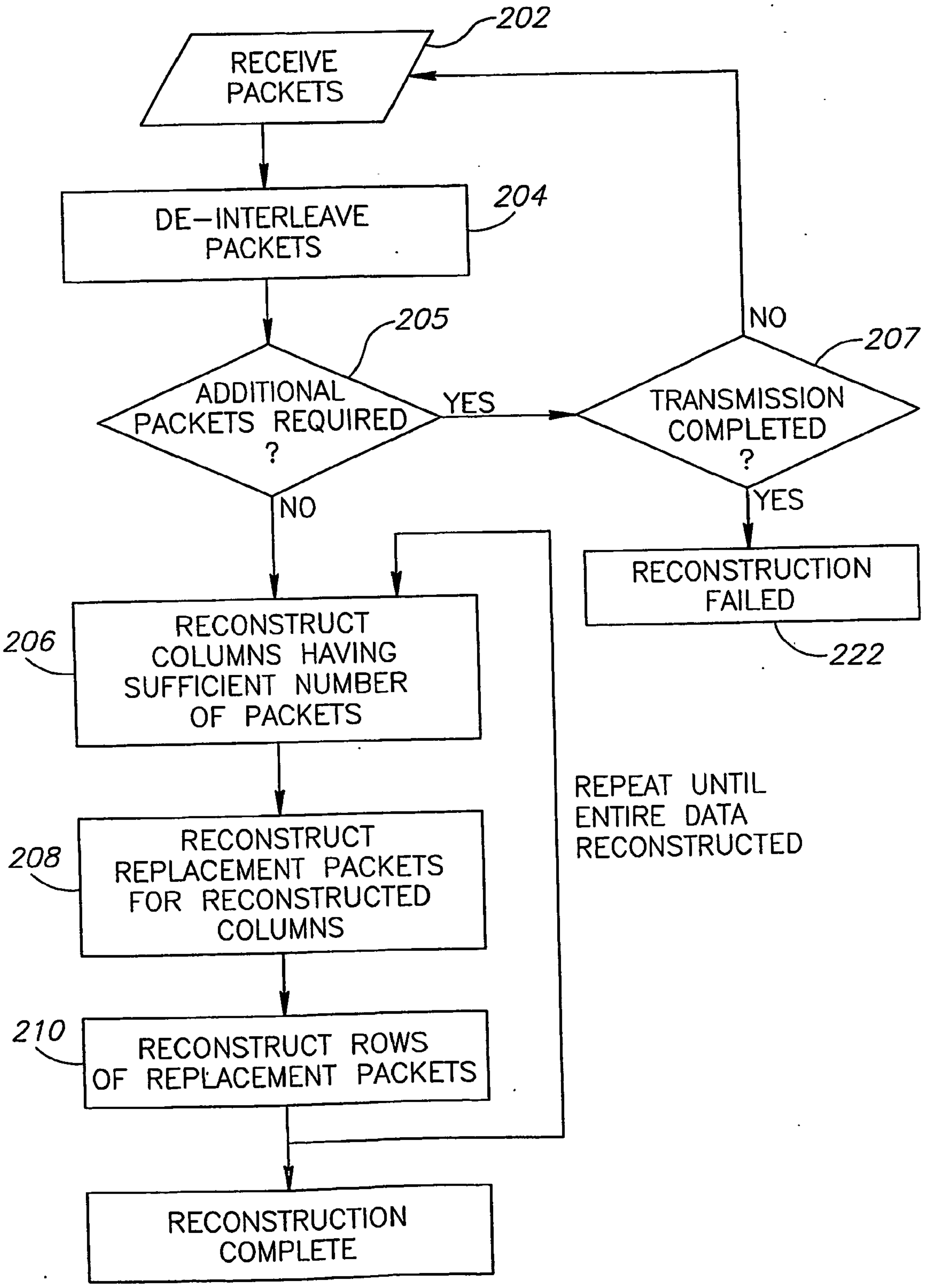
RECEIVE PACKETS
202
DE-INTERLEAVE PACKETS
204
ADDITIONAL PACKETS REQUIRED ?
205
YES
NO
TRANSMISSION COMPLETED ?
207
NO
YES
RECONSTRUCTION FAILED
222
RECONSTRUCT COLUMNS HAVING SUFFICIENT NUMBER OF PACKETS
206
RECONSTRUCT REPLACEMENT PACKETS FOR RECONSTRUCTED COLUMNS
208
RECONSTRUCT ROWS OF REPLACEMENT PACKETS
210
REPEAT UNTIL ENTIRE DATA RECONSTRUCTED
RECONSTRUCTION COMPLETE

FIG.2

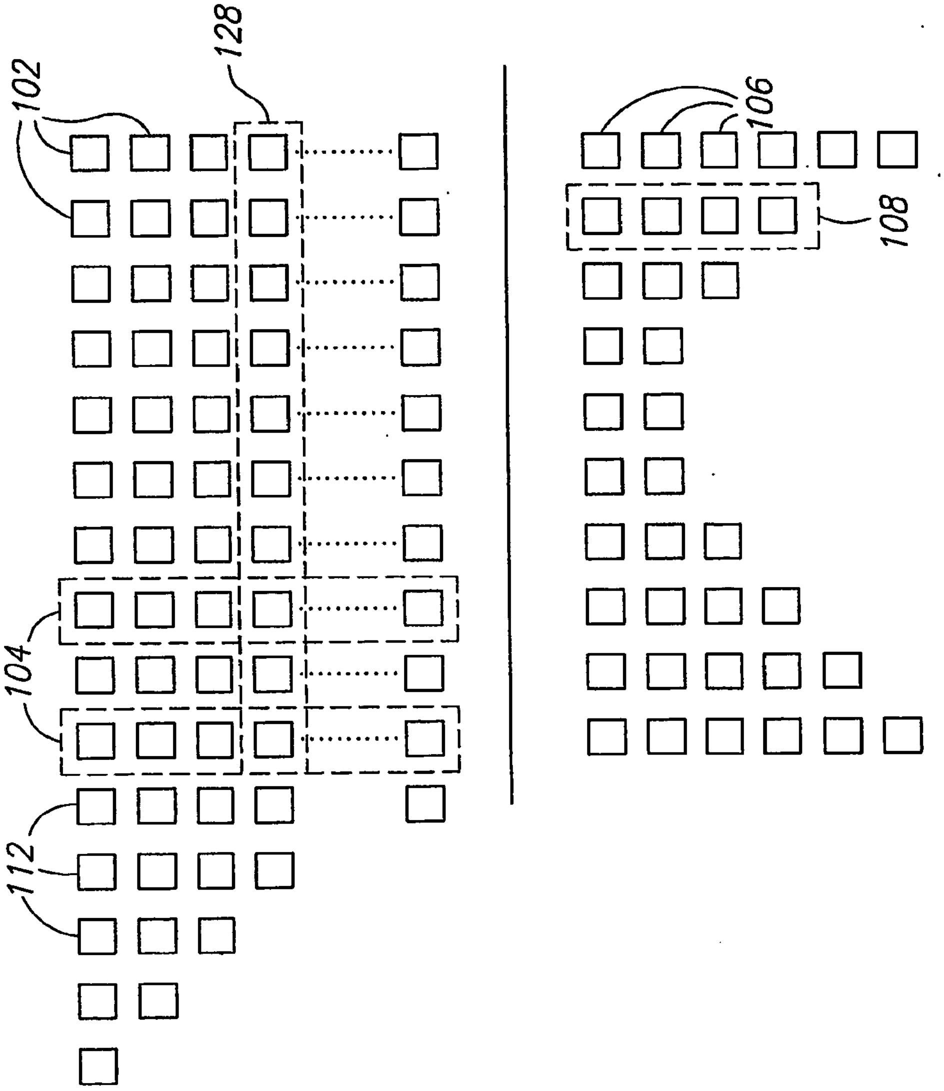

FIG.3